

MP W7100/W8140 series

Manuais do Utilizador

Guia de Segurança

Para uma utilização segura e correcta, certifique-se de que lê as Informações de Segurança em "Leia Este Documento Primeiro" antes de utilizar o equipamento.

CONTEÚDO

1. Para Começar a Utilizar o Equipamento

Antes de Configurar as Definições da Função de Segurança..... 9
Antes de Utilizar Este Equipamento..... 10
Administradores e Utilizadores..... 11
Administradores..... 12
Configurar a Autenticação dos Administradores..... 13
Especificar privilégios de administrador..... 14
Registar e alterar administradores..... 16
Utilizar o Web Image Monitor para configurar a autenticação de administrador..... 19
Método para Iniciar Sessão Como Administrador..... 20
Iniciar sessão utilizando o painel de controlo..... 20
Iniciar sessão utilizando o Web Image Monitor..... 21
Método para Encerrar Sessão Como Administrador..... 22
Encerrar sessão utilizando o painel de controlo..... 22
Encerrar sessão utilizando o Web Image Monitor..... 22
Supervisor..... 23
Repor a palavra-passe de administrador..... 23
Alterar o supervisor..... 24

2. Configurar a Autenticação dos Utilizadores

Utilizadores..... 27
Sobre a Autenticação de Utilizador..... 28
Configurar a Autenticação do Utilizador..... 29
Autenticação por Código de Utilizador..... 32
Autenticação Básica..... 34
Especificar a autenticação básica..... 34
Informações de autenticação guardadas no livro de endereços..... 36
Especificar nomes de utilizador e palavras-passe de início de sessão..... 36
Especificar detalhes de início de sessão..... 37
Autenticação Windows..... 39
Especificar a autenticação do Windows..... 41
Instalar os Internet Information Services (IIS) e Certificate Services..... 45
Criar o certificado de servidor..... 47
Autenticação LDAP..... 48

Autenticação de Trabalhos da Impressora....53
Níveis de autenticação de trabalhos da impressora....53
Tipos de trabalhos da impressora....54
Comando "authfree"....55
Registo Automático no Livro de Endereços....56
Itens registados automaticamente no livro de endereços....56
Defin transf dados p/programa auto livro endereços....56
Função de Bloqueio de Utilizadores....58
Especificar a função de bloqueio de utilizadores....59
Cancelar o bloqueio da palavra-passe....59
Encerramento Automático de Sessão....61
Autenticação Utilizando um Dispositivo Externo....63

3. Restringir a Utilização do Equipamento

Restringir Uso da Lista de Destinos....65
Impedir Alterações às Definições dos Administradores....67
Limitar as definições que podem ser alteradas por cada administrador....67
Proibir utilizadores de efetuar alterações às definições....67
Especificar a Função de Menu Protegido....68
Função de cópia....68
Função de impressora....68
Função de scanner....68
Impedir utilizadores de registar/alterar programas....69
Limitar as Funções Disponíveis....70
Restringir o Acesso à Slot para Dispositivos de Armazenamento Amovível....72

4. Prevenir Contra Fugas de Informação a partir de Equipamentos

Proteger o Livro de Endereços....73
Especificar permissões de acesso ao livro de endereços....73
Encriptar dados no livro de endereços....75
Encriptar Dados no Equipamento....77
Ativar as definições de encriptação....79
Efetuar cópia de segurança da chave de encriptação....81
Atualizar a chave de encriptação....82
Cancelar a encriptação de dados....83

Apagar Dados no Equipamento....85
Apagar auto memória....85
Apagar toda a memória....89

5. Segurança de Rede Avançada

Controlo de Acesso....95
Ativar e Desativar Protocolos....96
Ativar e desativar protocolos utilizando o painel de controlo....100
Ativar e desativar protocolos utilizando o Web Image Monitor....100
Especificar Níveis de Segurança da Rede....102
Especificar os níveis de segurança de rede utilizando o painel de controlo....102
Especificar o nível de segurança de rede utilizando o Web Image Monitor....103
Estado das funções em cada nível de segurança da rede....103
Proteger Vias de Comunicação com um Certificado de Dispositivo....107
Criar e instalar um certificado de dispositivo a partir do painel de controlo (certificado próprio)....107
Criar e instalar um certificado de dispositivo a partir do Web Image Monitor (certificado próprio)....108
Criar um certificado do dispositivo (emitido por uma autoridade de certificação)....109
Instalar um certificado de dispositivo (emitidos por uma autoridade de certificação)....110
Instalação de um certificado intermédio (emitido por uma autoridade de certificação)....111
Configurar as Definições SSL/TLS....112
Ativar SSL/TLS....113
Definição de utilizador para SSL/TLS....114
Definir modo de encriptação SSL/TLS....115
Ativar SSL para Ligações SMTP....116
Configurar S/MIME....118
Encriptação de e-mail....118
Juntar uma assinatura eletrónica....120
Verificar o período de validade do certificado....122
Configurar PDFs com Assinaturas Eletrónicas....124
Configurar Definições IPsec....125
Encriptação e autenticação por IPsec....126
Definições da chave de encriptação negociada automaticamente....127
Definições IPsec....127

Sequência de configuração das Definições da chave de encriptação negociada automaticamente..... 133
Comandos de definição telnet..... 138
Configurar a Autenticação IEEE 802.1X..... 144
Instalar um certificado externo..... 144
Selecionar o certificado do dispositivo..... 145
Itens de definição de IEEE 802.1X para Ethernet..... 145
Itens de definição de IEEE 802.1X para Wireless LAN..... 147
Encriptação SNMPv3..... 150
Encriptar Palavras-Passe Transmitidas..... 151
Especificar um código de encriptação do controlador..... 151
Especificar uma palavra-passe de Autenticação IPP..... 152
Definição da Encriptação de Autenticação Kerberos..... 154

6. Prevenir Contra a Fuga de Documentos

Gerir Pastas..... 157
Eliminar pastas..... 157
Alterar a palavra-passe de uma pasta..... 158
Desbloquear pastas..... 159
Gerir Ficheiros Guardados..... 161
Configurar permissões de acesso para cada ficheiro guardado..... 162
Alterar o proprietário de um documento..... 165
Configurar as permissões de acesso para cada utilizador referentes a ficheiros guardados..... 165
Especificar palavras-passe para ficheiros guardados..... 167
Desbloquear ficheiros guardados..... 168
Gerir Ficheiros de Impressão Bloqueada..... 170
Eliminar ficheiros de impressão bloqueada..... 170
Alterar a palavra-passe de um ficheiro de impressão bloqueada..... 172
Desbloquear um ficheiro de impressão bloqueada..... 173
Imprimir Informações do Utilizador no Papel..... 175

7. Gerir o Equipamento

Gerir Ficheiros de Registo..... 177
Utilizar o Web Image Monitor para Gerir Ficheiros de Registo..... 178
Registos que podem ser geridos utilizando o Web Image Monitor..... 178

Atributos dos registos que é possível transferir..... 185
Especificar as definições da recolha de registos..... 210
Transferir registos..... 211
Número de registos que podem ser mantidos no equipamento..... 212
Notas acerca do funcionamento quando o número de entradas de registo atinge o máximo..... 213
Registos de trabalhos de impressora..... 215
Eliminar todos os registos..... 216
Desativar a transferência de registos para o servidor de recolha de registos..... 217
Gerir Registos a Partir do Equipamento..... 218
Especificar as definições da recolha de registos..... 218
Desativar a transferência de registos para o servidor de recolha de registos..... 218
Especificar Apagar todos os registos..... 219
Gerir registos a partir do servidor de recolha de registos..... 219
Configurar o Ecrã Inicial para Utilizadores Individuais..... 220
Avisos sobre a utilização de ecrãs iniciais personalizados..... 220
Configurar as Definições do Browser..... 222
Precauções para utilizar a função de browser..... 222
Troubleshooting..... 223
Gerir Informações do Equipamento..... 224
Exportar informações do equipamento..... 225
Importar informações do equipamento..... 227
Importar periodicamente informações do equipamento..... 228
Importar manualmente o ficheiro de informações das definições do equipamento a partir de um servidor..... 229
Troubleshooting..... 230
Gerir o Livro de Endereços..... 233
Especificar a eliminação automática de dados do livro de endereços..... 233
Eliminar todos os dados do livro de endereços..... 233
Especificar as Funções de Segurança Avançadas..... 234
Outras Funções de Segurança..... 242
Função de Scanner..... 242
Estado do sistema..... 242
Verificar a validade do firmware..... 242

Restringir a Utilização por Parte de um Técnico de Assistência.....243
Informações Adicionais para Segurança Avançada.....244
Definições que pode configurar utilizando o painel de controlo.....244
Definições que pode configurar utilizando o Web Image Monitor.....246
Definições que pode configurar quando o IPsec está disponível/indisponível.....248

8. Resolução de Problemas

Se for Visualizada uma Mensagem.....251
Se Aparecer um Código de Erro.....253
Autenticação básica.....253
Autenticação Windows.....254
Autenticação LDAP.....259
Se Não For Possível Operar o Equipamento.....264

9. Lista de Privilégios de Operação para Definições

Como Ler.....269
Definições do Sistema.....270
Editar Página Principal.....280
Funções de Copiador/Servidor de Documentos.....281
Funções da Impressora.....286
Funções de Impressora.....287
Funções de Scanner.....291
Funções de Browser.....293
Definições de Função Avançada.....294
Web Image Monitor: Trabalho.....295
Web Image Monitor: Definições do dispositivo.....297
Web Image Monitor: Impressora.....307
Web Image Monitor: Scanner.....310
Web Image Monitor: Interface.....313
Web Image Monitor: Rede.....315
Web Image Monitor: Segurança.....319
Web Image Monitor: @Remote.....321
Web Image Monitor: Página web.....322
Web Image Monitor: Definições de função avançada.....323
Web Image Monitor: Livro de endereços.....324

Web Image Monitor: Central Address Book Management..... 325
Web Image Monitor: Main Power Off..... 326
Web Image Monitor: Apagar trabalho da impressora..... 327
Web Image Monitor: Reiniciar sistema..... 328
Web Image Monitor: Gestão da Página Principal..... 329
Web Image Monitor: Monitorização do ecrã..... 330
Web Image Monitor: Personalizar ecrã por utilizador..... 331
Web Image Monitor: Servidor de documentos..... 332
Web Image Monitor: Impressora: Trabalhos de impressão..... 333
Lista de Privilégios de Operação para Ficheiros Guardados..... 334
Lista de Privilégios de Operação para Livros de Endereços..... 336
ÍNDICE..... 339

1. Para Começar a Utilizar o Equipamento

Este capítulo descreve as precauções que necessita de tomar quando utilizar as funções de segurança do equipamento e explica como configurar as definições de administrador.

Antes de Configurar as Definições da Função de Segurança

Importante

- **Se as definições de segurança não estiverem configuradas, os dados no equipamento estarão vulneráveis a ataques.**
- Para impedir que este equipamento seja furtado ou intencionalmente danificado, instale-o num local seguro.
- Os proprietários deste equipamento devem assegurar uma utilização adequada por parte dos utilizadores, de acordo com as operações determinadas pelo administrador e supervisor do equipamento. Se o administrador ou o supervisor não efetuar as definições de segurança necessárias, existe o risco de brechas de segurança por parte dos utilizadores.
- Antes de definir as funções de segurança do equipamento e de assegurar uma utilização adequada por parte dos utilizadores, os administradores devem ler na íntegra o Guia de Segurança, prestando particular atenção ao capítulo intitulado "Antes de configurar as definições das funções de segurança".
- Os administradores têm de informar os utilizadores sobre a utilização correta das funções de segurança.
- Se este equipamento estiver ligado a uma rede, o seu ambiente tem de estar protegido por uma firewall ou semelhante.
- Para proteção de dados durante a fase de comunicação, aplique as funções de segurança de comunicação do equipamento e ligue-o a dispositivos que suportem funções como comunicação encriptada.
- Os administradores devem examinar regularmente os registos do equipamento para verificar se existem situações anormais.

Antes de Utilizar Este Equipamento

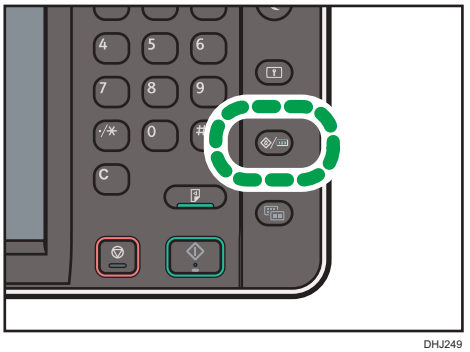
1

Esta secção explica como encriptar dados transmitidos e configurar a conta do administrador. Se pretende um nível elevado de segurança, efetue a seguinte definição antes de utilizar o equipamento.

1. **Ligue o equipamento.**

   Para mais detalhes sobre como ligar o equipamento, consulte Getting Started.

2. **Prima a tecla [Ferramentas do utilizador/Contador].**



3. **Prima [Definições do sistema].**
4. **Prima [Defin. interface].**
5. **Especifique o endereço IPv4.**

   Para mais informações sobre como especificar o endereço IPv4, consulte Connecting the Machine/ System Settings.

6. **Prima [Transfer. ficheiros] nas [Definições do sistema].**
7. **Prima [Endereço de e-Mail do administrador] e, em seguida, especifique o endereço de e-mail do administrador deste equipamento.**
8. **Crie e instale o certificado do dispositivo a partir do painel de controlo.**

   Para informações sobre como instalar o certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo".

   Introduza o endereço especificado no passo 7 como o endereço de e-mail para o certificado do dispositivo.

9. **Altere o nome de utilizador e a palavra-passe de início de sessão do administrador.**

   Para mais informações sobre como especificar nomes de utilizador e palavras-passe de início de sessão dos administradores, consulte Pág. 16 "Registar e alterar administradores".

10. **Ligue o equipamento ao ambiente de rede de utilização geral.**

Nota

- Para ativar um nível de segurança mais elevado, consulte Pág. 244 "Informações Adicionais para Segurança Avançada".

Administradores e Utilizadores

Esta secção explica os termos "administrador", "supervisor", "utilizador" e proprietário" tal como são utilizados neste manual.

Administrador

Existem 4 tipos de administradores do equipamento: administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros.

A sua principal função consiste em especificar as definições de utilização do equipamento. Os seus privilégios de acesso variam consoante o tipo de administrador. Os administradores não podem realizar operações habituais, como copiar e imprimir.

Supervisor

Existe apenas um supervisor. O supervisor pode especificar a palavra-passe de cada administrador. Não é necessário um supervisor para as operações habituais, uma vez que os administradores podem especificar as respetivas palavras-passe.

Utilizador

Os utilizadores são pessoas que utilizam o equipamento para realizar operações habituais, como copiar e imprimir.

Proprietário

Um proprietário é um utilizador que registou ficheiros no equipamento através das funções de copiador, impressora ou outra.

Administradores

Os administradores gerem o acesso do utilizador ao equipamento e várias outras funções e definições importantes.

Quando um administrador controlar o acesso limitado e as definições, selecione em primeiro lugar o administrador do equipamento e ative a função de autenticação antes de utilizar o equipamento. Quando a função de autenticação está ativada, são necessários o nome de utilizador e a palavra-passe de início de sessão para utilizar o equipamento. A função de administrador para este equipamento está dividida em 4 categorias de acordo com as respetivas funções: administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros. Partilhar tarefas facilita a tarefa de cada administrador e, ao mesmo tempo, evita operações não autorizadas de administrador. É possível atribuir várias funções de administrador a um administrador, do mesmo modo que uma função pode ser partilhada por mais do que um administrador. Também é possível definir um supervisor, o qual poderá então alterar as palavras-passe dos administradores.

Os administradores não podem utilizar funções como cópia e impressão. Para utilizar estas funções, o administrador tem de se autenticar como utilizador.

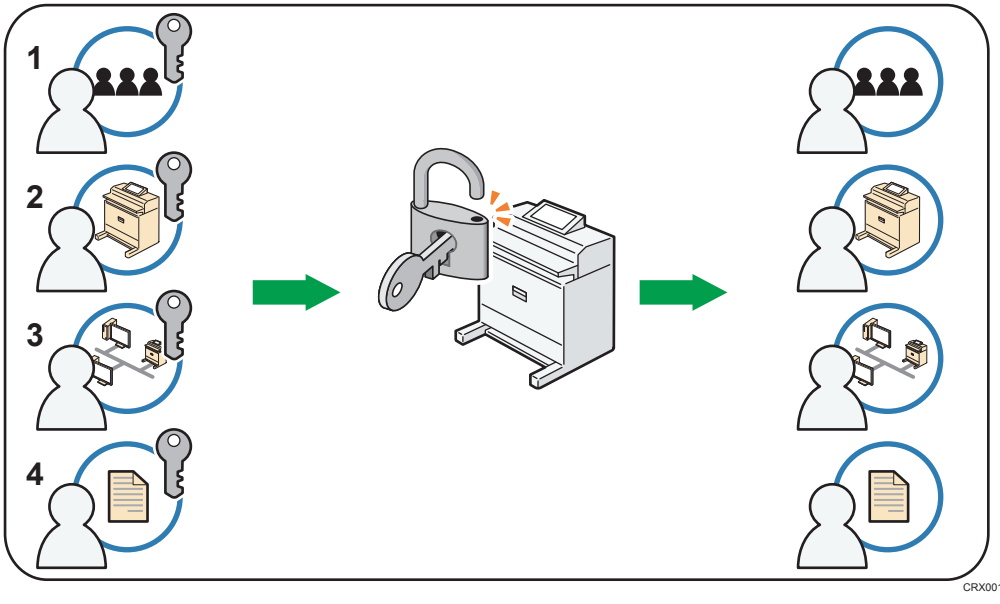
Para mais informações sobre como registar um administrador, consulte Pág. 16 "Registar e alterar administradores", e, para mais informações sobre como alterar a palavra-passe de um administrador, consulte Pág. 23 "Supervisor". Para mais informações sobre os utilizadores, consulte Pág. 27 "Utilizadores".

Configurar a Autenticação dos Administradores

A autenticação de administrador requer a introdução do nome de utilizador e palavra-passe para verificar os administradores que tentem especificar as definições do equipamento ou aceder às definições a partir de uma rede. Ao registar um administrador, não pode utilizar um nome de utilizador de início de sessão já registado no livro de endereços. Os administradores são geridos de forma diferente dos utilizadores registados no livro de endereços. A autenticação Windows e autenticação LDAP não são realizadas para um administrador para que um administrador possa iniciar sessão mesmo que o servidor não esteja acessível devido a um problema de rede. Cada administrador é identificado através de um nome de utilizador de início de sessão. Uma pessoa pode acumular funções de mais do que um tipo de administrador se forem atribuídos privilégios de vários administradores a um único nome de utilizador para início de sessão. Para instruções sobre como registar o administrador, consulte Pág. 16 "Registar e alterar administradores".

Pode especificar um nome de utilizador e uma palavra-passe para início de sessão e uma palavra--passe de encriptação para cada administrador. A palavra-passe de encriptação é utilizada para encriptar dados transmitidos através de SNMPv3. É também utilizada por aplicações como Device Manager NX, que utilizam o SNMPv3. Os administradores apenas podem gerir as definições do equipamento e controlar o acesso dos utilizadores e, como tal, não podem utilizar funções como copiar e imprimir. Para utilizar estas funções, o administrador tem de registar-se como utilizador no livro de endereços e autenticar-se. Especifique a autenticação de administrador e, em seguida, a autenticação de utilizador. Para mais informações sobre como especificar a autenticação, consulte Pág. 29 "Configurar a Autenticação do Utilizador".

As funções de cada administrador



1. **Administrador de utilizadores**

   Gere informações pessoais no livro de endereços.

   Um administrador de utilizadores pode registar/apagar utilizadores no livro de endereços ou alterar os dados pessoais dos utilizadores.

   Os utilizadores registados no livro de endereços também podem alterar e apagar os seus próprios dados pessoais.

   Se um utilizador se esquecer da sua palavra-passe, o administrador de utilizadores pode apagar essa palavra-passe e criar uma nova, permitindo ao utilizador aceder novamente ao equipamento.

2. **Administrador do equipamento**

   Gere essencialmente as predefinições do equipamento. Pode definir o equipamento para que as predefinições para cada função possam apenas ser especificadas pelo administrador do equipamento. Ao efetuar esta definição, pode evitar que utilizadores não autorizados alterem as definições e permitir que o equipamento seja utilizado com segurança pelos seus utilizadores.

3. **Administrador de rede**

   Gere as definições de rede. Pode definir o equipamento para que as definições da rede, como o endereço IP e as definições de envio e receção de e-mail, possam apenas ser especificadas pelo administrador da rede.

   Ao efetuar esta definição, pode evitar que pessoas não autorizadas alterem as definições e desativem o equipamento, garantindo assim o correto funcionamento da rede.

4. **Administrador de ficheiros**

   Gere as permissões de acesso a ficheiros guardados. Pode especificar palavras-passe para determinar que apenas utilizadores registados têm permissão para visualizar e editar ficheiros guardados no servidor de documentos. Utilizando esta definição, pode evitar a fuga e a alteração de dados devido a utilizadores não autorizados que visualizem e utilizem dados registados.

Nota

- A autenticação de administradores também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- Pode especificar a autenticação por código de utilizador sem especificar a autenticação de administrador.

Especificar privilégios de administrador

Para especificar a autenticação do administrador, defina "Gestão de autenticação do administrador" como [Ligado]. Se esta definição estiver ativada, os administradores podem configurar apenas definições alocadas aos próprios.

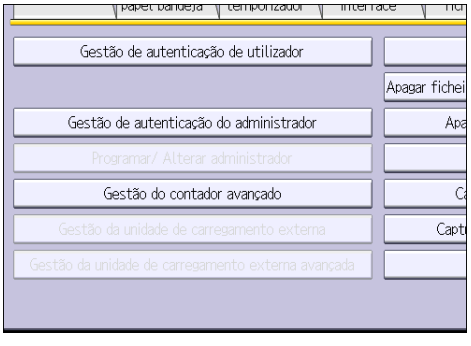
Para iniciar sessão como administrador, utilize o nome de utilizador e a palavra-passe de início de sessão predefinidos.

Para mais informações sobre como iniciar e encerrar sessão com autenticação de administrador, consulte Pág. 20 "Método para Iniciar Sessão Como Administrador" e Pág. 22 "Método para Encerrar Sessão Como Administrador".

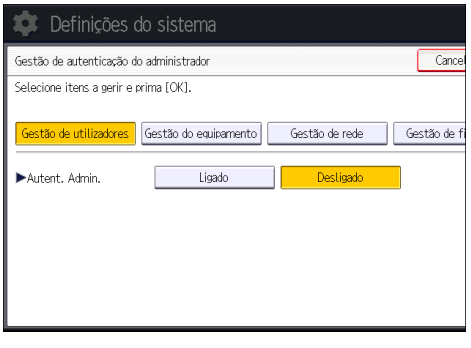
Importante

- Se tiver ativado a "Gestão de autenticação do administrador", certifique-se de que não se esquece do nome de utilizador e da palavra-passe de início de sessão do administrador. Se se esquecer do nome de utilizador ou da palavra-passe para início de sessão de um administrador, terá de ser especificada uma nova palavra-passe utilizando as credenciais de supervisor. Para mais informações sobre os privilégios do supervisor, consulte Pág. 23 "Supervisor".

1. Prima a tecla [Ferramentas do utilizador/Contador].
2. Prima [Definições do sistema].
3. Prima [Ferr. Administrador].
4. Prima [▼Seg.].
5. Prima [Gestão de autenticação do administrador].


Gestão de autenticação de utilizador
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

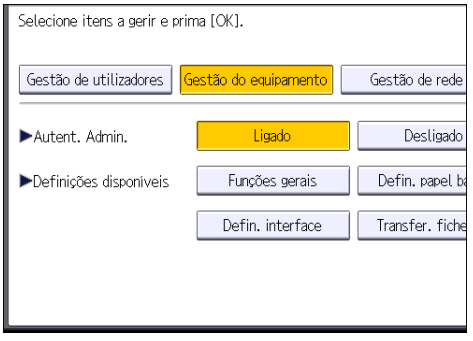
6. Prima [Gestão de utilizadores], [Gestão do equipamento], [Gestão de rede] ou [Gestão de ficheiros] para selecionar as definições a gerir.



7. Defina "Autent. Admin." como [Ligado].

   É visualizado "Definições disponíveis".

8. **Selecione as definições a gerir a partir de "Definições disponíveis".**



As definições selecionadas não estarão disponíveis para os utilizadores.

As definições disponíveis variam consoante o tipo de administrador.

Para especificar a autenticação de administrador para mais de uma categoria, repita os passos 6 a 8.

9. **Prima [OK].**
10. **Prima a tecla [Ferramentas do utilizador/Contador].**

Registar e alterar administradores

Se tiver especificado a autenticação de administrador, recomendamos que apenas uma pessoa assuma cada papel de administrador.

Partilhar tarefas facilita a tarefa de cada administrador e também evita operações não autorizadas de administrador. Pode registar até 4 nomes de utilizador para início de sessão (Administradores 1-4) aos quais pode conceder privilégios de administrador.

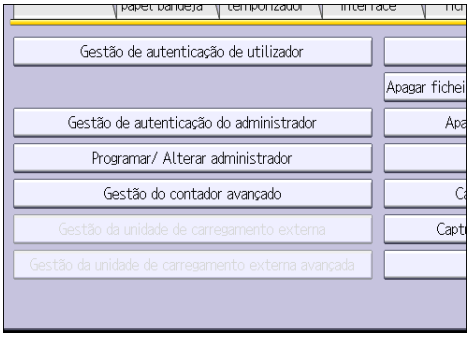
Os privilégios de um administrador só podem ser alterados por um administrador que tenha os privilégios relevantes.

Certifique-se de que atribui todos os privilégios de administrador de modo que cada privilégio de administrador fique associado, pelo menos, a um administrador.

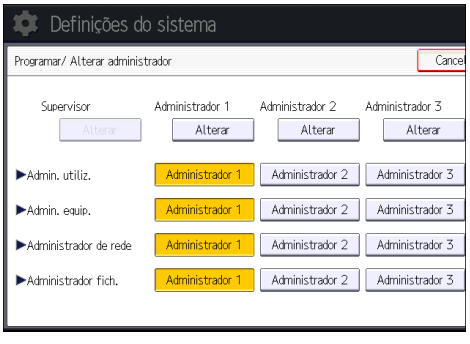
Para mais informações sobre como iniciar e encerrar sessão com autenticação de administrador, consulte Pág. 20 "Método para Iniciar Sessão Como Administrador" e Pág. 22 "Método para Encerrar Sessão Como Administrador".

1. **Inicie sessão como administrador no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**

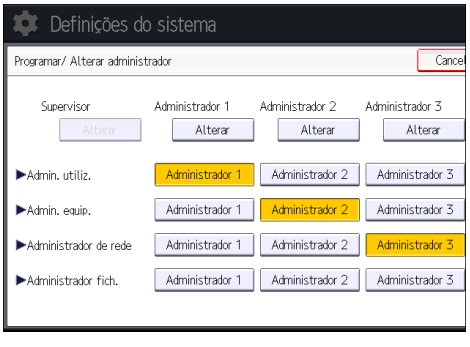
5. **Prima [Programar/ Alterar administrador].**


Gestão de autenticação de utilizador
Apagar fichei
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

6. **Na linha correspondente ao administrador cujos privilégios pretende especificar, prima [Administrador 1], [Administrador 2], [Administrador 3] ou [Administrador 4] e, em seguida, prima [Alterar].**



Quando atribuir privilégios de cada administrador individualmente, selecione um administrador para cada categoria, como indicado abaixo.



Para combinar vários privilégios de administrador, atribua vários privilégios de administrador a um único administrador.

Por exemplo, para atribuir privilégios de administrador do equipamento e privilégios de administrador de utilizadores ao [Administrador 1], prima [Administrador 1] nas linhas referentes ao administrador do equipamento e ao administrador de utilizadores.

7. **Prima [Alterar] para "Nome utiliz. início sessão".**

8. **Introduza o nome de utilizador de início de sessão e, em seguida, prima [OK].**
9. **Prima [Alterar] para "Pal-passe início sessão".**
10. **Introduza a palavra-passe de início de sessão e, em seguida, prima [OK].**

    Siga a política de palavras-passe para uma palavra-passe de início de sessão forte.

    Para mais informações sobre a política de palavras-passe e como especificá-la, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".
11. **Introduza novamente a palavra-passe de início de sessão para fins de confirmação e, em seguida, prima [OK].**
12. **Prima [Alterar] para "Pal.-passe de encriptação".**
13. **Introduza a palavra-passe de encriptação e, em seguida, prima [OK].**
14. **Introduza novamente a palavra-passe de encriptação para fins de confirmação e, em seguida, prima [OK].**
15. **Prima [OK] duas vezes.**

    A sessão será automaticamente encerrada.

Nota

- Para mais informações sobre os carateres que podem ser utilizados para os nomes de utilizador e palavras-passe para início de sessão, consulte Pág. 18 "Carateres utilizáveis para nomes de utilizador e palavras-passe".

Carateres utilizáveis para nomes de utilizador e palavras-passe

Os carateres seguintes podem ser utilizados para nomes de utilizador e palavras-passe de início de sessão. Nos nomes e nas palavras-passe distinguem-se maiúsculas de minúsculas.

- Maiúsculas: A a Z (26 carateres)
- Minúsculas: a a z (26 carateres)
- Números: 0 a 9 (10 carateres)
- Símbolos: (espaço) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 carateres)

Nome de utilizador de início de sessão

- Não pode conter espaços, dois pontos ou aspas.
- Não pode ficar em branco.
- O comprimento máximo é de 32 carateres.
- O nome de utilizador de um administrador para início de sessão tem de conter outros tipos de caráter que não carateres numéricos (números) se tiver até 8 carateres. Se contiver apenas números, têm de ser utilizados 9 ou mais.

Palavra-passe de início de sessão

- O comprimento máximo para as palavras-passe de administradores e supervisores é de 32 carateres e de 128 carateres para os utilizadores.
- Não existem quaisquer restrições aos tipos de carateres que podem ser utilizados para a palavra-passe. Para efeitos de segurança, é recomendado criar palavras-passe contendo carateres em maiúsculas e minúsculas, números e símbolos. Uma palavra-passe composta por muitos carateres é mais difícil de ser adivinhada por outros utilizadores.
- Em [Política de palavra-passe] sob [Segurança Avançada], pode especificar uma palavra--passe composta por maiúsculas e minúsculas, números e símbolos, bem como o número mínimo de carateres a utilizar para a palavra-passe. Para detalhes sobre como especificar a política de palavras-passe, consulte a respetiva secção em Pág. 234 "Especificar as Funções de Segurança Avançadas".

Utilizar o Web Image Monitor para configurar a autenticação de administrador

Utilizando o Web Image Monitor, pode iniciar a sessão no equipamento e alterar as definições do administrador. Para mais informações sobre como iniciar e encerrar sessão com autenticação de administrador, consulte Pág. 20 "Método para Iniciar Sessão Como Administrador" e Pág. 22 "Método para Encerrar Sessão Como Administrador".

1. **Inicie sessão como administrador a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Gestão de autenticação do administrador] ou em [Programar/Alterar administrador], sob "Definições do dispositivo".**
4. **Altere as definições conforme pretendido.**
5. **Encerre sessão.**

Nota

- Para mais informações sobre o Web Image Monitor, consulte a Ajuda do Web Image Monitor.

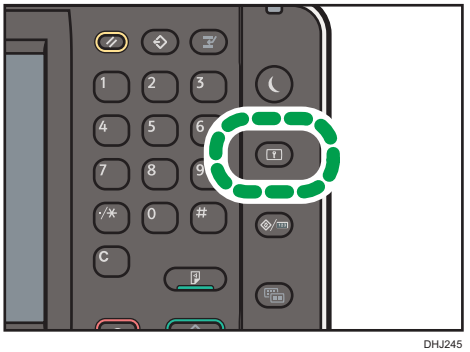
Método para Iniciar Sessão Como Administrador

Se tiver sido especificada a autenticação de administrador, inicie sessão utilizando um nome de utilizador e palavra-passe de início de sessão de administrador. Os supervisores iniciam sessão da mesma forma.

Para mais informações acerca do nome de utilizador e palavra-passe para o administrador e supervisor, pergunte o administrador.

Iniciar sessão utilizando o painel de controlo

1. **Prima a tecla [Ferramentas do utilizador/Contador].**
2. **Prima a tecla [Iniciar/Encerrar sessão].**

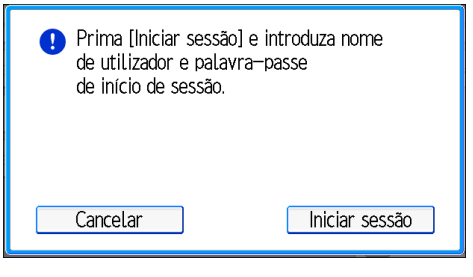


DHJ245

Aparece o ecrã de início de sessão.

O ecrã de início de sessão também pode ser chamado premindo [Iniciar sessão] no menu Ferramentas do utilizador.

3. **Prima [Iniciar sessão].**



4. **Introduza o nome de utilizador de início de sessão e, em seguida, prima [OK].**
5. **Introduza a palavra-passe de início de sessão e, em seguida, prima [OK].**

"A autenticar. . . Aguarde. " aparece, seguido do ecrã Ferramentas do utilizador.

Nota

- Se a autenticação de utilizador já tiver sido especificada, aparece um ecrã para autenticação. Para iniciar a sessão como administrador, introduza o nome de utilizador e a palavra-passe de início de sessão.
- Se iniciar sessão utilizando privilégios de administrador, é apresentado o nome do administrador a iniciar sessão. Quando iniciar sessão com um nome de utilizador com vários privilégios de administrador, é apresentado um dos privilégios associados a esse nome.
- Se tentar iniciar sessão a partir de um ecrã de operações, surge a mensagem "Não possui privilégios para utilizar esta função. Apenas pode alterar definições como administrador.". Prima a tecla [Ferramentas do utilizador/Contador] para apresentar o ecrã Ferramentas do utilizador.

Iniciar sessão utilizando o Web Image Monitor

1. **Abra um Web browser.**
2. **Introduza "http://(endereço da impressora)/" na barra de endereços.**

   Ao introduzir um endereço IPv4, não comece os segmentos com zeros. Por exemplo: se o endereço for "192.168.001.010", deve introduzi-lo como "192.168.1.10" para ligar ao equipamento.

   Introduza o endereço IPv6 dentro de parêntesis retos, desta forma: [2001:db8::9abc].

   Se definiu "Permitir comunicação SSL/TLS" para [Só texto cifrado], introduza " https://(endereço IP ou nome do sistema host do equipamento)/" para aceder ao equipamento.
3. **Clique em [Iniciar sessão] na parte superior direita da janela.**
4. **Introduza o nome de utilizador e a palavra-passe de início de sessão de um administrador e, em seguida, clique em [Iniciar sessão].**

Nota

- O web browser poderá estar configurado para preencher automaticamente as caixas de diálogo de início de sessão retendo os nomes de utilizador e as palavras-passe de início de sessão. Essa função diminui a segurança. Para evitar que o web browser retenha os nomes de utilizador e as palavras-passe de início de sessão, desative a função de preenchimento automático do browser.

Método para Encerrar Sessão Como Administrador

Se tiver sido especificada a autenticação de administrador, certifique-se de que encerra a sessão depois de concluir as alterações de definições. Os supervisores encerram sessão da mesma forma.

Encerrar sessão utilizando o painel de controlo

1. **Prima a tecla [Iniciar/Encerrar sessão] e, em seguida, prima [Sim].**

Nota

- Também pode encerrar a sessão utilizando os procedimentos que se seguem:
  - Prima a tecla [Poupança de energia].

Encerrar sessão utilizando o Web Image Monitor

1. **Clique em [Encerrar sessão] no canto superior direito da janela.**

Nota

- Depois de encerrar a sessão, limpe a cache no Web Image Monitor.

Supervisor

O supervisor pode apagar a palavra-passe de um administrador e especificar uma nova.

Se um administrador se esquecer ou alterar a sua palavra-passe, o supervisor pode atribuir uma nova palavra-passe ao administrador. Se iniciar sessão utilizando o nome de utilizador e a palavra-passe do supervisor, não pode utilizar as funções normais nem especificar definições de sistema. Os métodos para iniciar e encerrar sessão são os mesmos utilizados por administradores. Consulte Pág. 20 "Método para Iniciar Sessão Como Administrador" e Pág. 22 "Método para Encerrar Sessão Como Administrador".

Importante

- **Certifique-se de que não se esquece do nome de utilizador e da palavra-passe para iniciar sessão como supervisor. Caso se esqueça, um elemento da assistência técnica terá de repor o equipamento para o seu estado predefinido. Os dados de definição, os contadores, os registos e outros dados do equipamento serão perdidos. A chamada de assistência técnica poderá não ser gratuita.**

Nota

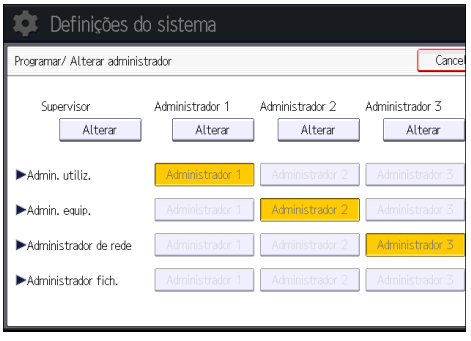
- Para mais informações sobre os carateres que podem ser utilizados para os nomes de utilizador e palavras-passe para início de sessão, consulte Pág. 18 "Carateres utilizáveis para nomes de utilizador e palavras-passe".
- Não pode especificar o mesmo nome de utilizador de início de sessão para o supervisor e os administradores.
- Utilizando o Web Image Monitor, pode iniciar sessão como supervisor e apagar a palavra-passe de um administrador ou especificar uma nova.

Repor a palavra-passe de administrador

1. **Inicie sessão como supervisor no painel de controlo.**

   Para mais informações sobre como iniciar sessão, consulte Pág. 20 "Método para Iniciar Sessão Como Administrador".
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Programar/ Alterar administrador].**

6. **Prima [Alterar] para o administrador que pretende repor.**



7. **Prima [Alterar] para "Pal-passe início sessão".**
8. **Introduza a palavra-passe de início de sessão e, em seguida, prima [OK].**
9. **Introduza novamente a palavra-passe de início de sessão para fins de confirmação e, em seguida, prima [OK].**
10. **Prima [OK] duas vezes.**

    A sessão será automaticamente encerrada.

Nota

- O supervisor pode alterar as palavras-passe de início de sessão dos administradores mas não os respetivos nomes de utilizador.

Alterar o supervisor

Este capítulo descreve como alterar o nome de utilizador e palavra-passe de início de sessão do supervisor.

Para fazê-lo, tem de ativar os privilégios do administrador de utilizador através das definições em "Gestão de autenticação do administrador". Para mais informações, consulte Pág. 14 "Especificar privilégios de administrador".

1. **Inicie sessão como supervisor no painel de controlo.**

   Para mais informações sobre como iniciar sessão, consulte Pág. 20 "Método para Iniciar Sessão Como Administrador".
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Programar/ Alterar administrador].**
6. **Em "Supervisor", prima [Alterar].**
7. **Prima [Alterar] para "Nome utiliz. início sessão".**

8. **Introduza o nome de utilizador de início de sessão e, em seguida, prima [OK].**
9. **Prima [Alterar] para "Pal-passe início sessão".**
10. **Introduza a palavra-passe de início de sessão e, em seguida, prima [OK].**
11. **Introduza novamente a palavra-passe de início de sessão para fins de confirmação e, em seguida, prima [OK].**
12. **Prima [OK] duas vezes.**

    A sessão será automaticamente encerrada.

2. Configurar a Autenticação dos Utilizadores

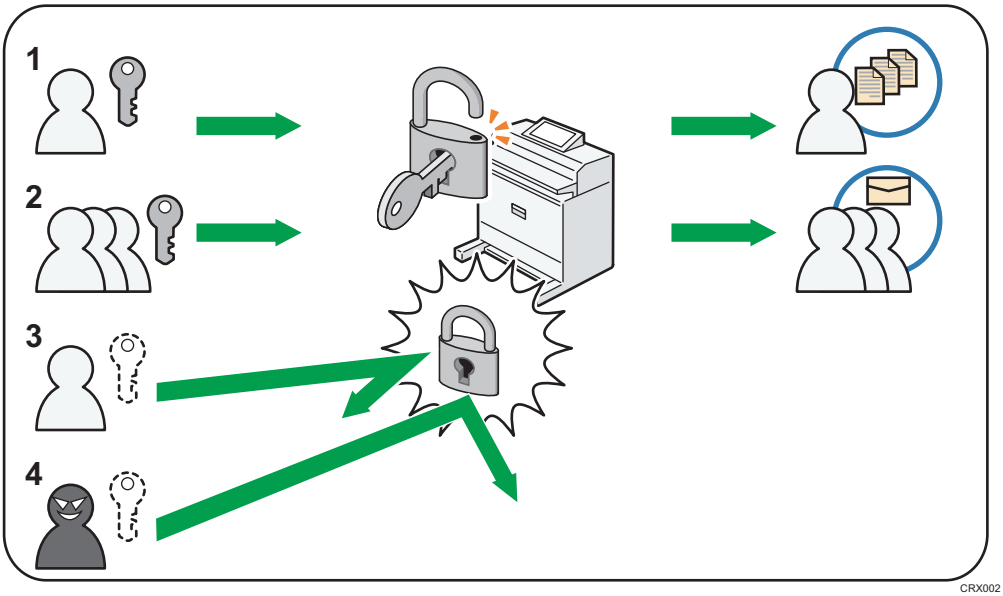
Este capítulo descreve como especificar a autenticação de utilizador e explica as funções que são ativadas pela autenticação de utilizador.

Utilizadores

Um utilizador efetua operações normais no equipamento, tais como copiar e imprimir. Os utilizadores são geridos de acordo com as informações pessoais no livro de endereços do equipamento e apenas podem utilizar as funções que lhes são permitidas pelo acesso definido pelos administradores. Ativando a autenticação de utilizador, pode permitir que apenas pessoas registadas no livro de endereços utilizem o equipamento. Os utilizadores podem ser geridos no livro de endereços pelo administrador de utilizadores. Para mais informações sobre os administradores, consulte Pág. 12 "Administradores". Para detalhes sobre o registo de utilizadores no livro de endereços, consulte Connecting the Machine/ System Settings ou a Ajuda do Web Image Monitor.

Sobre a Autenticação de Utilizador

A autenticação de utilizadores é um sistema que requer nome de utilizador e palavra-passe para início de sessão para verificar os utilizadores que podem utilizar o equipamento ou aceder ao equipamento através da rede.



1. **Utilizador**

   Um utilizador efetua operações normais no equipamento, tais como copiar e imprimir.

2. **Grupo**

   Um grupo efetua operações normais no equipamento, tais como copiar e imprimir.

3. **Utilizador não autorizado**

4. **Acesso não autorizado**

Configurar a Autenticação do Utilizador

Existem 4 tipos de métodos de autenticação de utilizador: autenticação por código de utilizador, autenticação básica, autenticação Windows e autenticação LDAP. Para utilizar a autenticação de utilizador, selecione um método de autenticação no painel de controlo e, em seguida, efetue as definições necessárias para a autenticação. As definições dependem do método de autenticação. Especifique a autenticação de administrador e, em seguida, a autenticação de utilizador.

Importante

- **Se não for possível ativar a autenticação do utilizador devido a um problema com o disco rígido ou com a rede, pode utilizar o equipamento efetuando o acesso através da autenticação de administrador e desativando a autenticação de utilizador. Proceda desta forma se, por exemplo, tiver de utilizar o equipamento com urgência.**
- **Não pode utilizar mais do que um método de autenticação ao mesmo tempo.**

Sequência de configuração da autenticação do utilizador

Procedimento de configuração	Detalhes
Configurar a autenticação do administrador	Pág. 14 "Especificar privilégios de administrador" Pág. 16 "Registar e alterar administradores"
Configurar a autenticação do utilizador	Especifique a autenticação do utilizador. Estão disponíveis 4 tipos de autenticação de utilizador: • Pág. 32 "Autenticação por Código de Utilizador" • Pág. 34 "Autenticação Básica" • Pág. 39 "Autenticação Windows" • Pág. 48 "Autenticação LDAP"

Métodos de autenticação dos utilizadores

Tipo	Detalhes
Autenticação através do código de utilizador	A autenticação é realizada através de códigos de utilizador de oito dígitos. A autenticação é aplicada a cada código de utilizador, não a cada utilizador. É necessário registar previamente o código de utilizador no livro de endereços do equipamento.

Tipo	Detalhes
Autenticação básica	A autenticação é realizada através do livro de endereços do equipamento. É necessário registar previamente os utilizadores no livro de endereços do equipamento. A autenticação pode ser aplicada a cada utilizador.
Autenticação Windows	A autenticação é realizada através da controladora de domínio do servidor Windows ligado à mesma rede do equipamento. A autenticação pode ser aplicada a cada utilizador.
Autenticação LDAP	A autenticação é realizada através do servidor LDAP ligado à mesma rede do equipamento. A autenticação pode ser aplicada a cada utilizador.

É possível utilizar um endereço de e-mail de um utilizador obtido via autenticação Windows ou LDAP como endereço fixo do remetente ("De") ao enviar e-mails no modo de scanner de forma a prevenir a usurpação de ID.

Se o método de autenticação dos utilizadores for entretanto alterado

- É possível transferir e utilizar como nome de utilizador para início de sessão uma conta de código de utilizador que não tenha mais de 8 dígitos e que seja utilizada para autenticação por código de utilizador, mesmo depois de o método de autenticação mudar de autenticação por código de utilizador para autenticação básica, autenticação Windows ou autenticação LDAP. Nesse caso, uma vez que não é fornecida uma palavra-passe para a autenticação de código de utilizador, a palavra-passe de início de sessão fica em branco.
- Se o método de autenticação mudar para autenticação externa (autenticação Windows ou autenticação LDAP), a autenticação não pode ser ativada, a não ser que a conta de código de utilizador transferida tenha sido previamente registada no dispositivo de autenticação externa. No entanto, a conta de código de utilizador será guardada no livro de endereços do equipamento mesmo que ocorra uma falha de autenticação.
- Do ponto de vista da segurança, se o método de autenticação mudar de autenticação por código de utilizador para outro tipo de autenticação, é aconselhável eliminar contas que já não sejam utilizadas ou configurar uma palavra-passe para início de sessão. Para mais informações sobre como eliminar contas, consulte Connecting the Machine/ System Settings. Para mais informações sobre como alterar palavras-passe, consulte Pág. 36 "Especificar nomes de utilizador e palavras-passe de início de sessão".

Nota

- Após ligar a alimentação, as funcionalidades avançadas podem não aparecer na lista de itens de autenticação de utilizador no menu Gestão de autenticação de utilizador. Se isto acontecer, aguarde um momento e abra novamente o menu Gestão de autenticação de utilizador
- A autenticação de utilizador também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

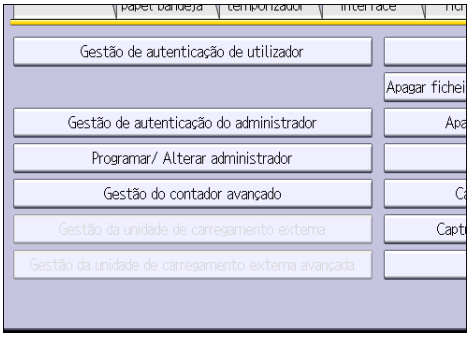
Autenticação por Código de Utilizador

Este é um método de autenticação para limitar o acesso a funções de acordo com um código de utilizador. O mesmo código de utilizador pode ser utilizado por vários utilizadores.

Para detalhes sobre como especificar códigos de utilizador, consulte Connecting the Machine/ System Settings.

Para detalhes sobre como especificar o código de utilizador no driver de impressão ou driver TWAIN, consulte a Ajuda do driver.

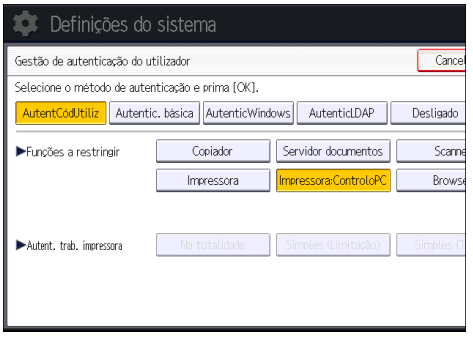
1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Gestão de autenticação de utilizador].**


Gestão de autenticação de utilizador
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

6. **Selecione [AutentCódUtiliz].**

   Se não pretender ativar a autenticação de utilizador, selecione [Desligado].

7. **Em "Funções a restringir", selecione as funções que pretende restringir.**



As funções selecionadas estão sujeitas a autenticação por código de utilizador. A autenticação por código de utilizador não se aplica às funções não selecionadas.

Para mais informações sobre como limitar as funções disponíveis para utilizadores individuais ou grupos, consulte Pág. 70 "Limitar as Funções Disponíveis".

8. **Em "Funções a restringir", anule a seleção [Impressora:ControloPC] ou selecione [Impressora].**

   Se não pretender especificar a autenticação dos trabalhos de impressora, avance para o passo 13.

9. **Selecione o nível de "Autent. trab. impressora".**

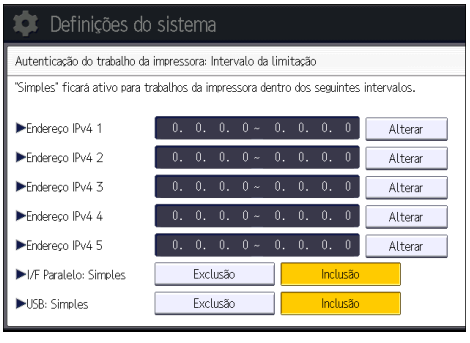
   Para uma descrição dos níveis de autenticação dos trabalhos de impressora, consulte Pág. 53 "Autenticação de Trabalhos da Impressora".

   Se selecionar [Na totalidade] ou [Simples (Todos)], avance para o passo 13.

   Se selecionar [Simples (Limitação)] , avance para o passo 10.

10. **Prima [Alterar] para "Intervalo do limite".**

11. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autent. trab. impressora".**


Definições do sistema
Autenticação do trabalho da impressora: Intervalo da limitação
"Simples" ficará ativo para trabalhos da impressora dentro dos seguintes intervalos.
▶Endereço IPv4 1
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 2
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 3
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 4
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 5
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶I/F Paralelo: Simples
Exclusão
Inclusão
▶USB: Simples
Exclusão
Inclusão

   Pode especificar o intervalo de endereços IPv4 ao qual pretende aplicar esta definição. Também pode especificar se pretende aplicar esta definição ao interface USB.

12. **Prima [Sair].**

13. **Prima [OK].**

14. **Prima a tecla [Iniciar/Encerrar sessão].**

    É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

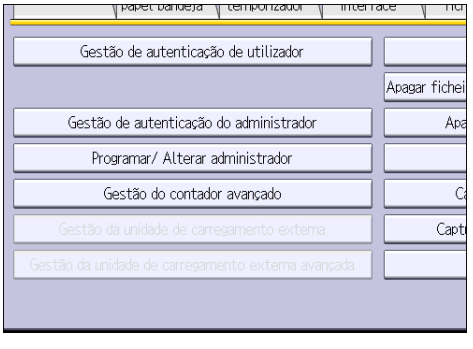
Autenticação Básica

Especifique este método de autenticação quando utilizar o livro de endereços do equipamento para autenticar cada utilizador. Utilizando a autenticação básica, pode não só gerir as funções disponíveis do equipamento, como também limitar o acesso a ficheiros guardados e ao livro de endereços. Na autenticação básica, o administrador tem de especificar as funções disponíveis a cada utilizador registado no livro de endereços. Para mais informações sobre como limitar funções, consulte Pág. 36 "Informações de autenticação guardadas no livro de endereços".

Especificar a autenticação básica

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador está corretamente configurada em "Gestão de autenticação do administrador".

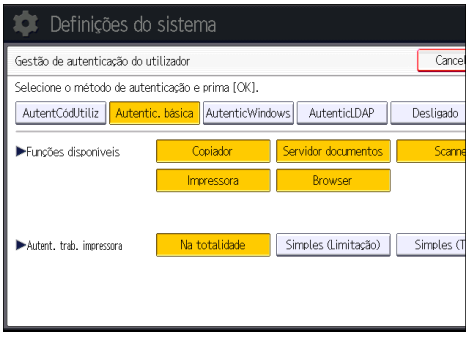
1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Gestão de autenticação de utilizador].**


Gestão de autenticação de utilizador
Apagar fichei
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

6. **Selecione [Autentic. básica].**

   Se não pretender ativar a autenticação de utilizador, selecione [Desligado].

7. **Em "Funções disponíveis", selecione que funções do equipamento pretende permitir.**



As funções que selecionar aqui tornam-se nas predefinições da autenticação básica que serão atribuídas a todos os novos utilizadores do livro de endereços.

Para mais informações sobre como especificar as funções disponíveis para utilizadores individuais ou grupos, consulte Pág. 70 "Limitar as Funções Disponíveis".

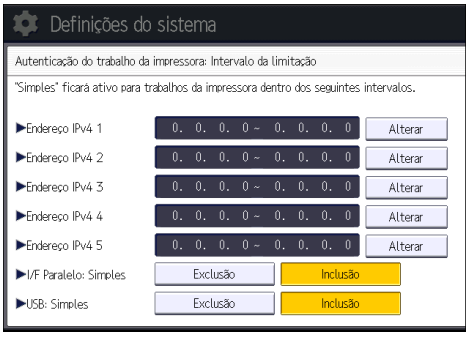
8. **Selecione o nível de "Autent. trab. impressora".**

Para uma descrição dos níveis de autenticação dos trabalhos de impressora, consulte Pág. 53 "Autenticação de Trabalhos da Impressora".

Se selecionar [Na totalidade] ou [Simples (Todos)], avance para o passo 12.

Se selecionar [Simples (Limitação)], avance para o passo 9.

9. **Prima [Alterar] para "Intervalo do limite".**
10. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autent. trab. impressora".**



Pode especificar o intervalo de endereços IPv4 ao qual pretende aplicar esta definição. Também pode especificar se pretende aplicar esta definição ao interface USB.

11. **Prima [Sair].**
12. **Prima [OK].**

13. **Prima a tecla [Iniciar/Encerrar sessão].**

    É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Informações de autenticação guardadas no livro de endereços

Se ativou a autenticação de utilizador, pode especificar os limites de acesso e de utilização para as funções do equipamento para cada utilizador ou grupo de utilizadores. Especifique as definições necessárias relativamente a cada utilizador no livro de endereços. Para mais informações sobre as funções que podem ser limitadas, consulte Pág. 70 "Limitar as Funções Disponíveis".

Os utilizadores devem ter uma conta registada no livro de endereços para utilizar o equipamento quando é especificada a autenticação de utilizador. Para detalhes sobre o registo de utilizadores no livro de endereços, consulte Connecting the Machine/ System Settings.

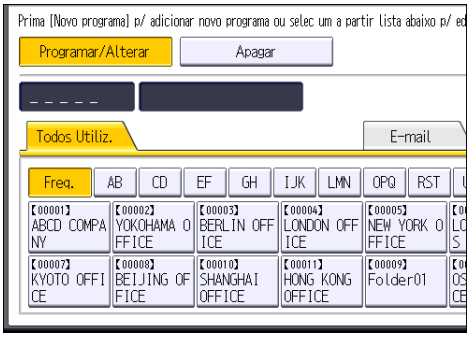
A autenticação de utilizador também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Especificar nomes de utilizador e palavras-passe de início de sessão

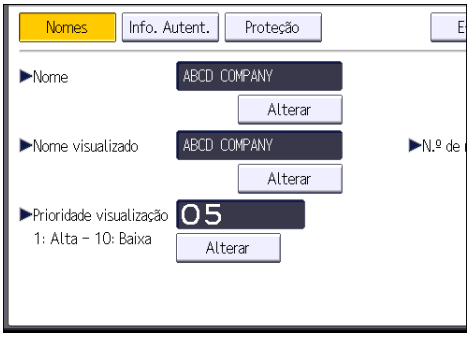
Em "Gestão do livro de endereços", especifique o nome de utilizador e a palavra-passe de início de sessão a serem utilizados para "Gestão de autenticação do utilizador".

Para mais informações sobre os carateres que podem ser utilizados para os nomes de utilizador e palavras-passe para início de sessão, consulte Pág. 18 "Carateres utilizáveis para nomes de utilizador e palavras-passe".

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Gestão livro de endereços].**
3. **Selecione o utilizador.**



4. **Prima [Info. Autent.].**



5. **Prima [Alterar] para "Nome utiliz. início sessão".**
6. **Introduza um nome de utilizador de início de sessão e, em seguida, prima [OK].**
7. **Prima [Alterar] para "Pal-passe início sessão".**
8. **Introduza uma palavra-passe de início de sessão e, em seguida, prima [OK].**
9. **Introduza novamente a palavra-passe de início de sessão para fins de confirmação e, em seguida, prima [OK].**
10. **Prima [OK].**
11. **Prima [Sair].**
12. **Encerre sessão.**

Especificar detalhes de início de sessão

O nome de utilizador e a palavra-passe de início de sessão especificados em "Gestão do livro de endereços" podem ser utilizados como informação de início de sessão para "Autenticação SMTP", "Autenticação da pasta" e "Autenticação LDAP".

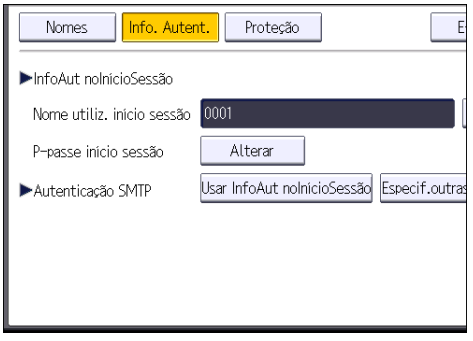
Se não pretender utilizar o nome de utilizador e a palavra-passe de início de sessão especificados em "Gestão do livro de endereços" para "Autenticação SMTP", "Autenticação da pasta" ou "Autenticação LDAP", consulte Connecting the Machine/ System Settings.

Importante

- **Quando utilizar "Usar InfoAut noInícioSessão" para "Autenticação SMTP", "Autenticação da pasta" ou "Autenticação LDAP", tem de ser especificado um nome diferente de "other", "admin", "supervisor" ou "HIDE***". O símbolo "***" representa qualquer caráter.**

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Gestão livro de endereços].**
3. **Selecione o utilizador.**
4. **Prima [Info. Autent.].**

5. **Selecione [Usar InfoAut noInícioSessão] em "Autenticação SMTP".**



Para autenticação da pasta, selecione [Usar InfoAut noInícioSessão] em "Autenticação da pasta".

Para autenticação LDAP, selecione [Usar InfoAut noInícioSessão] em "Autenticação LDAP".

Se a função que pretende selecionar não for apresentada, prima [▼Seg.].

6. **Prima [OK].**
7. **Prima [Sair].**
8. **Encerre sessão.**

Autenticação Windows

Especifique esta autenticação quando utilizar a controladora de domínio do Windows para autenticar os utilizadores que têm as suas contas no servidor de diretório. Os utilizadores não podem ser autenticados se não tiverem conta no servidor de diretórios. Com a autenticação Windows, pode especificar o limite de acesso para cada grupo registado no servidor de diretórios. O livro de endereços guardado no servidor de diretórios pode ser registado no equipamento, permitindo a autenticação do utilizador sem utilizar primeiro o equipamento para registar as definições individuais no livro de endereços.

A primeira vez que aceder ao equipamento, pode utilizar as funções disponíveis para o seu grupo. Se não estiver registado num grupo, pode utilizar as funções disponíveis sob "*Grupo predefinido". Para limitar as funções que estão disponíveis para determinados utilizadores, efetue previamente as definições no livro de endereços.

Para registar automaticamente as informações do utilizador na autenticação Windows, é aconselhável encriptar a comunicação entre o equipamento e a controladora de domínio com SSL. Para o fazer, tem de criar um certificado de servidor para a controladora de domínio. Para mais informações sobre como criar um certificado de servidor, consulte Pág. 47 "Criar o certificado de servidor".

Importante

- **Se utilizar a autenticação Windows, as informações do utilizador registadas no servidor de diretório são registadas automaticamente no livro de endereços do equipamento. Mesmo que as informações do utilizador registadas no livro de endereços do equipamento sejam editadas no equipamento, são substituídas pelas informações do servidor de diretório quando a autenticação for executada.**
- **Os utilizadores geridos em outros domínios estão sujeitos à autenticação de utilizador, mas não podem obter itens como, por exemplo, o nome do utilizador.**
- **Se forem definidas a autenticação Kerberos e a encriptação SSL ao mesmo tempo, não é possível obter endereços de e-mail.**
- **Se tiver criado um novo utilizador no controlador de domínio e tiver selecionado "O utilizador tem de alterar a palavra-passe no próximo início de sessão" na configuração da palavra-passe, primeiro inicie sessão no computador e, em seguida, altere a palavra-passe.**
- **Se o servidor de autenticação apenas suportar NTLM quando a autenticação Kerberos for selecionada no equipamento, o método de autenticação mudará automaticamente para NTLM.**
- **Se a conta "Convidado" no servidor Windows estiver ativa, os utilizadores não registados na controladora de domínio podem ser autenticados. Quando esta conta está ativada, os utilizadores são registados no livro de endereços e podem utilizar as funções disponíveis em "*Grupo predefinido".**

A autenticação Windows pode ser executada utilizando um de dois métodos de autenticação: autenticação NTLM ou Kerberos. Os requisitos operacionais para ambos os métodos são listados abaixo:

Requisitos operacionais para a autenticação NTLM

Para especificar a autenticação NTLM, devem ser cumpridos os seguintes requisitos:

- Este equipamento suporta a autenticação NTLMv1 e NTLMv2.
- Configure uma controladora de domínio no domínio que pretende usar.
- Esta função é suportada pelos sistemas operativos listados em seguida. Para obter informações do utilizador quando o Active Directory estiver a ser executado, utilize LDAP. Se utilizar LDAP, recomendamos que use SSL para encriptar a comunicação entre o equipamento e o servidor LDAP. A encriptação SSL é possível apenas se o servidor LDAP suportar TLSv1 ou SSLv3.
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

Requisitos operacionais para a autenticação Kerberos

Para especificar a autenticação Kerberos, devem ser cumpridos os seguintes requisitos:

- Configure uma controladora de domínio no domínio que pretende usar.
- O sistema operativo tem de suportar KDC (Key Distribution Center). Para obter informações do utilizador quando o Active Directory estiver a ser executado, utilize LDAP. Se utilizar LDAP, recomendamos que use SSL para encriptar a comunicação entre o equipamento e o servidor LDAP. A encriptação SSL é possível apenas se o servidor LDAP suportar TLSv1 ou SSLv3. Os sistemas operativos compatíveis são listados abaixo:
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

  Para utilizar a autenticação Kerberos no Windows Server 2008, instale o Service Pack 2 ou mais recente.
- A transmissão de dados entre o equipamento e o servidor KDC é encriptada se a autenticação Kerberos estiver ativada. Para mais informações sobre como especificar transmissões encriptadas, consulte Pág. 154 "Definição da Encriptação de Autenticação Kerberos".

Nota

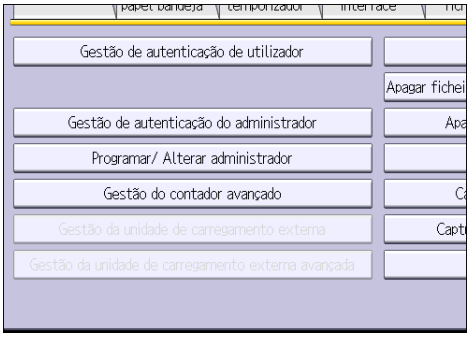
- Para mais informações sobre os carateres que podem ser utilizados para os nomes de utilizador e palavras-passe para início de sessão, consulte Pág. 18 "Carateres utilizáveis para nomes de utilizador e palavras-passe".
- Quando aceder posteriormente ao equipamento, pode utilizar todas as funções disponíveis para o seu grupo e para si como utilizador individual.
- Os utilizadores que estão registados em vários grupos podem utilizar todas as funções disponíveis para esses grupos.

- Com a autenticação Windows, não necessita criar um certificado de servidor, a menos que queira registar automaticamente informações de utilizadores, como nomes de utilizadores com SSL.

Especificar a autenticação do Windows

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador está corretamente configurada em "Gestão de autenticação do administrador".

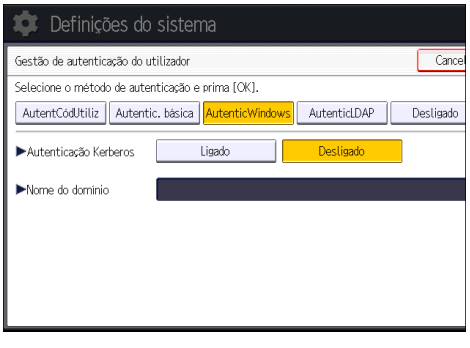
1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Gestão de autenticação de utilizador].**


Gestão de autenticação de utilizador
Apagar fichei
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

6. **Selecione [AutenticWindows].**

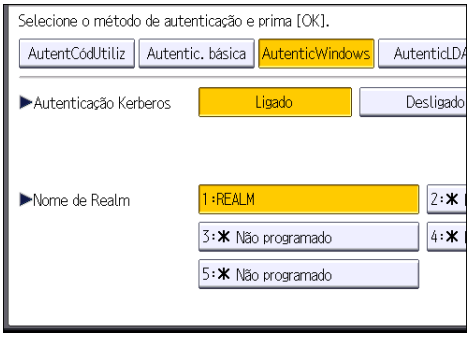
   Se não pretender ativar a autenticação de utilizador, selecione [Desligado].

7. **Se pretender utilizar a autenticação Kerberos, prima [Ligado].**



   Se pretender utilizar a autenticação NTLM, prima [Desligado] e avance para o passo 9.

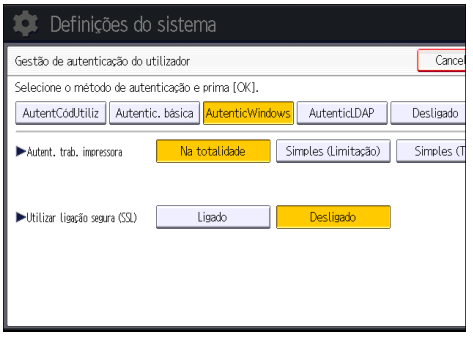
8. **Selecione o realm de autenticação Kerberos e avance para o passo 10.**



Para ativar a autenticação Kerberos, é necessário registar previamente um realm. É necessário registar um nome do realm em maiúsculas. Para mais informações acerca do registo de um realm, consulte Connecting the Machine/ System Settings.

É possível registar até 5 realms.

9. **Prima [Alterar] para "Nome do domínio", introduza o nome da controladora de domínio a autenticar e, em seguida, prima [OK].**
10. **Prima [▼Seg.].**
11. **Selecione o nível de "Autent. trab. impressora".**

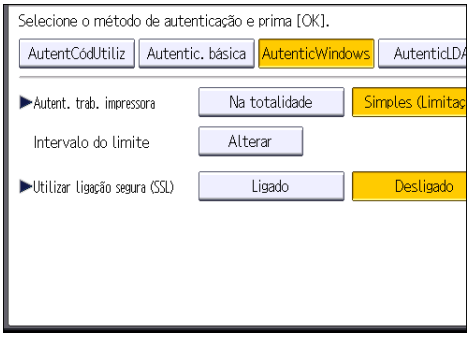


Para uma descrição dos níveis de autenticação dos trabalhos de impressora, consulte Pág. 53 "Autenticação de Trabalhos da Impressora".

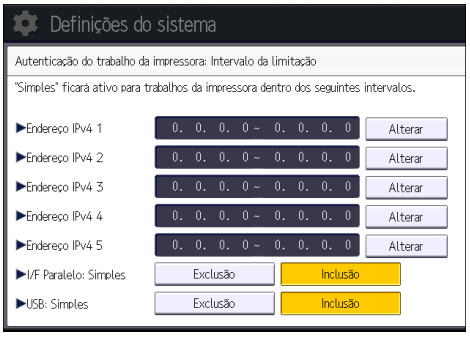
Se selecionar [Na totalidade] ou [Simples (Todos)], avance para o passo 15.

Se selecionar [Simples (Limitação)] , avance para o passo 12.

12. **Prima [Alterar].**



13. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autent. trab. impressora".**



Pode especificar o intervalo de endereços IPv4 ao qual pretende aplicar esta definição. Também pode especificar se pretende aplicar esta definição ao interface USB.

14. **Prima [Sair].**

15. **Prima [Ligado] para "Utilizar ligação segura (SSL)".**

Se não utilizar Secure Sockets Layer (SSL) na autenticação, prima [Desligado].

Se não tiver registado um grupo global, avance para o passo 22.

Se tiver registado um grupo global, avance para o passo 16.

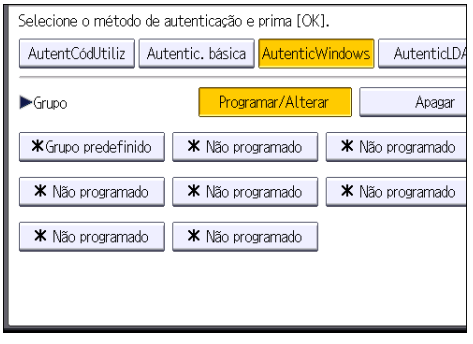
Se tiverem sido registados grupos globais no servidor do Windows, pode limitar a utilização de funções para cada grupo global.

É necessário criar antecipadamente grupos globais no servidor do Windows e registar em cada grupo os utilizadores a serem autenticados. Também é necessário registar no equipamento as funções disponíveis para os membros do grupo global. Crie grupos globais no equipamento introduzindo os nomes dos grupos globais registados no Servidor Windows. (Tenha em conta que nos nomes dos grupos distinguem-se maiúsculas de minúsculas.) Em seguida, especifique as funções do equipamento disponíveis para cada grupo.

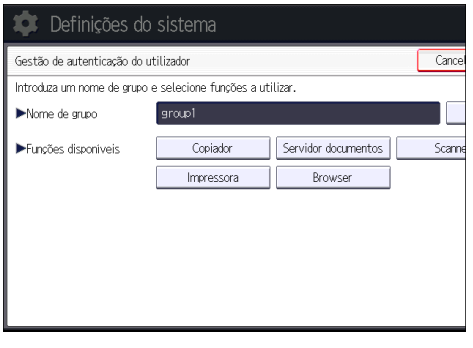
Se não estiverem especificados grupos globais, os utilizadores podem utilizar as funções especificadas em [*Grupo predefinido]. Se estiverem especificados grupos globais, os

utilizadores não registados em grupos globais podem utilizar as funções especificadas em [*Grupo predefinido]. Por predefinição, todas as funções estão disponíveis para membros do *Grupo predefinido. Especifique a limitação das funções disponíveis consoante as necessidades dos utilizadores.

16. **Prima [▼Seg.].**
17. **Em "Grupo", prima [Programar/Alterar] e, em seguida, prima [* Não programado].**



18. **Prima [Alterar] para "Nome de grupo" e introduza o nome do grupo.**
19. **Prima [OK].**
20. **Em "Funções disponíveis", selecione que funções do equipamento pretende permitir.**



A autenticação Windows será aplicada às funções selecionadas.

Os utilizadores só podem utilizar as funções selecionadas.

Para mais informações sobre como especificar as funções disponíveis para utilizadores individuais ou grupos, consulte Pág. 70 "Limitar as Funções Disponíveis".

21. **Prima [OK].**
22. **Prima [OK].**
23. **Prima a tecla [Iniciar/Encerrar sessão].**

É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Instalar os Internet Information Services (IIS) e Certificate Services

Especifique esta definição se pretender que o equipamento obtenha automaticamente informações de utilizador registados no Active Directory.

Recomendamos que instale Internet Information Services (IIS) e Certificate services como componentes do Windows.

Instale os componentes e crie o certificado de servidor.

Se não estiverem instalados, instale-os do seguinte modo:

Instalação com o Windows Server 2008 R2

1. **No menu [Iniciar], vá a [Ferramentas de administrador] e, em seguida, clique em [Gestor de servidores].**
2. **Clique em [Funções] na coluna esquerda e clique em [Adicionar funções] a partir do menu [Ação].**
3. **Clique em [Seguinte>].**
4. **Selecione as caixas "Servidor Web (IIS)" e "Serviços de Certificados do Active Directory" e, em seguida, clique em [Seguinte>].**

   Se surgir uma mensagem de confirmação, clique em [Adicionar funcionalidades].
5. **Leia as informações do conteúdo e, em seguida, clique em [Seguinte>].**
6. **Verifique se [Autoridade de certificação] está selecionada e, em seguida, clique em [Seguinte>].**
7. **Selecione [Empresa] e, em seguida, clique em [Seguinte>].**
8. **Selecione [AC de Raiz] e, em seguida, clique em [Seguinte>].**
9. **Selecione [Criar uma nova chave privada] e, em seguida, clique em [Seguinte>].**
10. **Selecione um fornecedor de serviços criptográficos, o comprimento da chave e o algoritmo hash para criar uma nova chave privada e, em seguida, clique em [Seguinte>].**
11. **Em "Nome comum para esta AC:", introduza o nome da autoridade de certificação e, em seguida, clique em [Seguinte>].**
12. **Selecione o período de validade e, em seguida, clique em [Seguinte>].**
13. **Coloque as definições da "Localização da base de dados de certificados:" e da "Localização do registo da base de dados de certificados:" nas respetivas predefinições e, em seguida, clique em [Seguinte>].**
14. **Leia as notas e, em seguida, clique em [Seguinte>].**
15. **Selecione o serviço da função que pretende utilizar e, em seguida, clique em [Seguinte>].**
16. **Clique em [Instalar].**

17. **Quando a instalação estiver concluída, clique em [Fechar].**
18. **Feche o [Gestor de servidores].**

Instalação com o Windows Server 2012

1. **No ecrã Iniciar, clique em [Gestor de servidores].**
2. **No menu [Gerir], clique em [Adicionar funções e funcionalidades].**
3. **Clique em [Seguinte>].**
4. **Selecione [Instalação baseada na função ou na funcionalidade] e clique em [Seguinte>].**
5. **Selecione um servidor e, em seguida, clique em [Seguinte>].**
6. **Selecione as caixas "Serviços de certificados do Active Directory" e "Servidor Web (IIS)" e, em seguida, clique em [Seguinte>].**

   Se surgir uma mensagem de confirmação, clique em [Adicionar funcionalidades].
7. **Selecione as funcionalidades que pretende instalar e clique em [Seguinte>].**
8. **Leia as informações do conteúdo e, em seguida, clique em [Seguinte>].**
9. **Certifique-se de que a opção [Autoridade de certificação] está selecionada na área [Serviços das funções], em [Serviços de certificados do Active Directory], e clique em [Seguinte>].**
10. **Leia as informações do conteúdo e, em seguida, clique em [Seguinte>].**
11. **Selecione os serviços de funções que pretende instalar com o [Servidor Web (IIS)], e, em seguida, clique em [Seguinte>].**
12. **Clique em [Instalar].**
13. **Após concluir a instalação, clique no ícone de notificação do Gestor de servidores e, em seguida, clique em [Configurar serviços de certificados do Active Directory no servidor de destino].**
14. **Clique em [Seguinte>].**
15. **Clique em [Autoridade de certificação] na área de [Serviços de funções] e seguidamente em [Seguinte>].**
16. **Selecione [AC da Empresa] e, em seguida, clique em [Seguinte>].**
17. **Selecione [AC de Raiz] e, em seguida, clique em [Seguinte>].**
18. **Selecione [Criar uma nova chave privada] e, em seguida, clique em [Seguinte>].**
19. **Selecione um fornecedor criptográfico, o comprimento da chave e o algoritmo hash para criar uma nova chave privada e, em seguida, clique em [Seguinte>].**
20. **Em "Nome comum para esta AC:", introduza o nome da autoridade de certificação e, em seguida, clique em [Seguinte>].**
21. **Selecione o período de validade e, em seguida, clique em [Seguinte>].**

22. **Coloque as definições da "Localização da base de dados de certificados:" e da "Localização do registo da base de dados de certificados:" nas respetivas predefinições e, em seguida, clique em [Seguinte>].**
23. **Clique em [Configurar].**
24. **Se surgir a mensagem "Configuração bem-sucedida", clique em [Fechar].**

Criar o certificado de servidor

Depois de instalar os componentes do Windows Serviços de informação Internet (IIS) e Serviços de certificados, crie o certificado de servidor do seguinte modo:

O Windows Server 2008 R2 é utilizado para mostrar o procedimento.

1. **No menu [Iniciar], vá a [Ferramentas de administrador] e, em seguida, clique em [Gestor de Serviços de Informação Internet (IIS)].**

   Com o Windows Server 2012, clique em [Gestor de Serviços de Informação Internet (IIS)] no ecrã Iniciar.

   Quando aparecer a mensagem de confirmação, clique em [Sim].
2. **Na coluna da esquerda, clique no nome do servidor e, em seguida, clique duas vezes em [Certificados de Servidor].**
3. **Na coluna direita, clique em [Criar Requisição de Certificado...].**
4. **Introduza toda as informações e, em seguida, clique em [Seguinte].**
5. **Em "Fornecedor de serviços criptográficos:", selecione um fornecedor e, em seguida, clique em [Seguinte].**
6. **Clique em [...] e, em seguida, especifique um nome de ficheiro para o pedido de certificado.**
7. **Especifique uma localização onde guardar o ficheiro e, em seguida, clique em [Abrir].**
8. **Feche o [Gestor de Serviços de Informação Internet (IIS)] clicando em [Concluir].**

Autenticação LDAP

Especifique este método de autenticação quando utilizar o servidor LDAP para autenticar utilizadores que tenham as suas contas no servidor LDAP. Os utilizadores não podem ser autenticados se não tiverem as suas contas no servidor LDAP. O livro de endereços guardado no servidor LDAP pode ser registado no equipamento, permitindo a autenticação do utilizador sem primeiro utilizar o equipamento para registar definições individuais no livro de endereços. Quando utilizar a autenticação LDAP, para evitar que a informação da palavra-passe seja enviada sem encriptação pela rede, recomendamos a encriptação da comunicação entre o equipamento e o servidor LDAP utilizando SSL. Pode especificar no servidor LDAP se pretende ou não ativar o SSL. Para o fazer, tem de criar um certificado de servidor para o servidor LDAP. Para mais informações sobre como criar um certificado de servidor, consulte Pág. 47 "Criar o certificado de servidor". As definições SSL podem ser especificadas na definição do servidor LDAP.

Utilizando o Web Image Monitor, pode ativar uma função para verificar a fiabilidade do servidor SSL. Para mais informações sobre a especificação da autenticação LDAP utilizando o Web Image Monitor, consulte a Ajuda do Web Image Monitor.

Quando seleciona autenticação de texto simples, é ativada a autenticação simplificada LDAP. A autenticação simplificada pode ser realizada com um atributo de utilizador (tal como cn ou uid), em vez de DN.

Para ativar Kerberos para a autenticação LDAP, é necessário registar previamente um realm. O realm tem de ser configurado em letras maiúsculas. Para mais informações acerca do registo de um realm, consulte Connecting the Machine/ System Settings.

Importante

- **Se utilizar autenticação LDAP, as informações de utilizador registadas no servidor LDAP são automaticamente registadas no livro de endereços do equipamento. Mesmo que as informações do utilizador registadas automaticamente no livro de endereços do equipamento sejam editadas no equipamento, serão substituídas pelas informações do servidor LDAP quando a autenticação for executada.**
- **Com a autenticação LDAP, não pode especificar limites de acesso para grupos registados no servidor do diretório.**
- **Não utilize carateres japoneses, chineses tradicionais, chineses simplificados ou coreanos de dois bytes quando introduzir o nome de utilizador ou a palavra-passe para início de sessão. Se utilizar carateres de vários bytes quando introduzir o nome de utilizador e palavra-passe para início de sessão, não pode autenticar-se utilizando o Web Image Monitor.**
- **Se utilizar o Active Directory na autenticação LDAP quando a autenticação Kerberos e SSL estiverem definidas ao mesmo tempo, não será possível obter informações dos utilizadores.**
- **Na autenticação LDAP, se a "Autenticação anónima" não estiver definida como "Proibir", os utilizadores que não têm conta no servidor LDAP podem aceder ao servidor.**

- **Se o servidor LDAP estiver configurado utilizando o Windows Active Directory, a "Autenticação anónima" poderá estar disponível. Se a autenticação Windows estiver disponível, recomendamos que a utilize.**

Requisitos operacionais para a autenticação LDAP

Para especificar a autenticação LDAP, devem ser cumpridos os seguintes requisitos:

- Configure a rede para que o equipamento possa detetar o servidor LDAP.
- Quando utilizar o SSL, o TLSv1 ou o SSLv3 podem ser executados no servidor LDAP.
- Registe o servidor LDAP no equipamento.
- Para registar o servidor LDAP, especifique as seguintes definições:
  - Nome servidor
  - Base de busca
  - Nº porta
  - Comunicação SSL
  - Autenticação

    Selecione a autenticação Kerberos, DIGEST ou autenticação de texto simples.
  - Nome do utilizador

    Não precisa de introduzir o nome de utilizador se o servidor LDAP suportar "Autenticação Anónima".
  - Palavra-passe

    Não precisa de introduzir a palavra-passe se o servidor LDAP suportar "Autenticação Anónima".

Para mais informações sobre como registar um servidor LDAP, consulte Connecting the Machine/ System Settings.

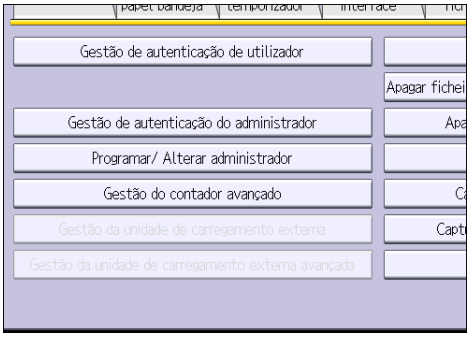
Nota

- Para mais informações sobre os carateres que podem ser utilizados para os nomes de utilizador e palavras-passe para início de sessão, consulte Pág. 18 "Carateres utilizáveis para nomes de utilizador e palavras-passe".
- No modo de autenticação simples LDAP, a autenticação falha se a palavra-passe for deixada em branco. Para utilizar palavras-passe em branco, contacte a assistência técnica.
- Da primeira vez que um utilizador não registado acede ao equipamento após a especificação da autenticação LDAP, o utilizador fica registado no equipamento e pode utilizar as funções disponíveis em "Funções disponíveis" durante a autenticação LDAP. Para limitar as funções disponíveis a cada utilizador, registe cada utilizador e a definição das "Funções disponíveis" correspondentes no livro de endereços ou especifique as "Funções disponíveis" para cada utilizador registado. A definição das "Funções disponíveis" é ativada quando o utilizador acede ao equipamento.

- A transmissão de dados entre o equipamento e o servidor KDC é encriptada se a autenticação Kerberos estiver ativada. Para mais informações sobre como especificar transmissões encriptadas, consulte Pág. 154 "Definição da Encriptação de Autenticação Kerberos".

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador está corretamente configurada em "Gestão de autenticação do administrador".

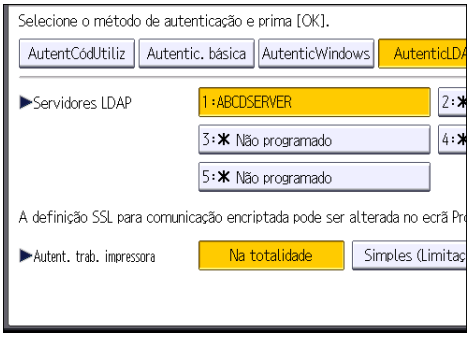
1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Gestão de autenticação de utilizador].**


Gestão de autenticação de utilizador
Apagar fichei
Gestão de autenticação do administrador
Programar/ Alterar administrador
Gestão do contador avançado
Gestão da unidade de carregamento externa
Gestão da unidade de carregamento externa avançada

6. **Selecione [AutenticLDAP].**

   Se não pretender ativar a autenticação de utilizador, selecione [Desligado].

7. **Selecione o servidor LDAP a utilizar para a autenticação LDAP.**



8. **Selecione o nível de "Autent. trab. impressora".**

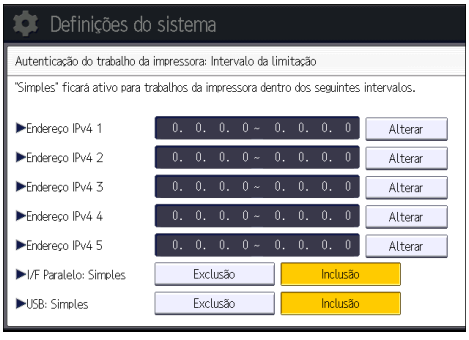
   Para uma descrição dos níveis de autenticação dos trabalhos de impressora, consulte Pág. 53 "Autenticação de Trabalhos da Impressora".

   Se selecionar [Na totalidade] ou [Simples (Todos)], avance para o passo 12.

   Se selecionar [Simples (Limitação)], avance para o passo 9.

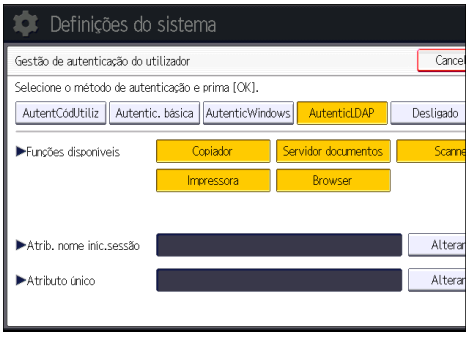
9. **Prima [Alterar] para "Intervalo do limite".**

10. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autent. trab. impressora".**


Definições do sistema
Autenticação do trabalho da impressora: Intervalo da limitação
"Simples" ficará ativo para trabalhos da impressora dentro dos seguintes intervalos.
▶Endereço IPv4 1
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 2
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 3
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 4
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶Endereço IPv4 5
0. 0. 0. 0 ~ 0. 0. 0. 0
Alterar
▶I/F Paralelo: Simples
Exclusão
Inclusão
▶USB: Simples
Exclusão
Inclusão

Pode especificar o intervalo de endereços IPv4 ao qual pretende aplicar esta definição. Também pode especificar se pretende aplicar esta definição ao interface USB.

11. **Prima [Sair].**
12. **Prima [▼Seg.].**
13. **Em "Funções disponíveis", selecione que funções do equipamento pretende permitir.**



A autenticação LDAP será aplicada às funções selecionadas.

Os utilizadores só podem utilizar as funções selecionadas.

Para mais informações sobre como especificar as funções disponíveis para utilizadores individuais ou grupos, consulte Pág. 70 "Limitar as Funções Disponíveis".

14. **Prima [Alterar] para "Atrib. nome iníc.sessão".**
15. **Introduza o atributo do nome de início de sessão e, em seguida, prima [OK].**

Utilize o atributo do nome de início de sessão como critério de procura para obter informações sobre um utilizador autenticado. Pode criar um filtro de procura com base no atributo do nome de início de sessão, selecionar um utilizador e, em seguida, obter as informações do utilizador a partir do servidor LDAP para que sejam transferidas para o livro de endereços do equipamento.

Para especificar vários atributos de início de sessão, coloque uma vírgula (,) entre eles. A procura devolverá correspondências de um ou de ambos os atributos.

Além disso, se colocar um sinal de igual (=) entre dois atributos de início de sessão (por exemplo: cn=abcde, uid=xyz), a procura só devolverá correspondências que coincidam com os atributos. Esta função de procura também pode ser aplicada quando a autenticação Texto Simples estiver especificada.

Quando autenticar utilizando o formato DN, os atributos de início de sessão não precisam de ser registados.

O método para selecionar o nome de utilizador depende do ambiente do servidor. Verifique o ambiente do servidor e introduza o nome do utilizador correspondente.

16. **Prima [Alterar] para "Atributo único".**
17. **Introduza o atributo único e, em seguida, prima [OK].**

    Especifique o atributo único no equipamento para fazer corresponder as informações do utilizador no servidor LDAP com as informações no equipamento. Ao fazê-lo, se o atributo único de um utilizador registado no servidor LDAP corresponder ao de um utilizador registado no equipamento, ambos os casos são tratados como referindo-se ao mesmo utilizador.

    Pode introduzir um atributo como “NúmeroSérie” ou “uid”. Pode ainda introduzir “cn” ou “NúmeroFuncionário”, desde que seja único. Se não especificar o atributo único, será criada no equipamento uma conta com as mesmas informações de utilizador mas com um nome de utilizador de início de sessão diferente.
18. **Prima [OK].**
19. **Prima a tecla [Iniciar/Encerrar sessão].**

    É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Autenticação de Trabalhos da Impressora

A autenticação do trabalho da impressora é uma função para aplicar a autenticação de utilizadores aos trabalhos de impressão.

Os drivers de impressão HDI e PostScript 3 e a Web Printing Tool suportam apenas a autenticação por código de utilizador.

Níveis de autenticação de trabalhos da impressora

O nível de segurança de "Na totalidade" é o mais elevado, seguido de "Simples (Limitação)" e, por fim, "Simples (Todos)".

- Na totalidade

  Selecione esta opção para autenticar todos os trabalhos de impressão e as definições remotas.

  O equipamento autentica todos os trabalhos da impressora e as definições remotas, cancelando os trabalhos e as definições cuja autenticação falhar.

  Para imprimir num ambiente que não suporte autenticação, selecione [Simples (Todos)] ou [Simples (Limitação)].

- Simples (Limitação)

  Selecione esta opção para restringir o intervalo de [Simples (Todos)].

  O intervalo especificado pode ser impresso independentemente da autenticação. A autenticação será aplicada aos endereços fora deste intervalo.

  Pode especificar a aplicação de [Simples (Todos)] para uma ligação USB e para o endereço IPv4 do utilizador. O intervalo da aplicação a endereços IPv6 pode ser configurado através do Web Image Monitor.

- Simples (Todos)

  Especifique esta definição se pretender imprimir com um driver de impressão ou um dispositivo que não possa ser identificado pelo equipamento ou se não precisar de autenticação para imprimir.

  Os trabalhos da impressora e as definições sem informações de autenticação são executados sem serem autenticados.

  O equipamento autentica os trabalhos da impressora e as definições remotas que possuam informações de autenticação, cancelando os trabalhos e as definições cuja autenticação falhar.

  Utilizadores não autorizados poderão utilizar o equipamento porque é permitida a impressão sem autenticação de utilizador.

Tipos de trabalhos da impressora

Dependendo da combinação do nível de autenticação do trabalho da impressora e do tipo de trabalho na impressora, o equipamento pode não imprimir corretamente. Defina uma combinação adequada de acordo com o ambiente de funcionamento.

Quando a autenticação do utilizador estiver desativada, a impressão está disponível para todos os tipos de trabalhos.

Tipos de trabalhos da impressora: É especificado um trabalho da impressora quando:

1. A caixa de seleção [Autenticação do utilizador] está selecionada no driver de impressão RP--GL/2.
2. A caixa de seleção [Autenticação do utilizador] não está selecionada no driver de impressão RP-GL/2.
3. Quando o código de utilizador é introduzido utilizando o driver de impressão PostScript 3, o driver universal PS3, a Web Printing Tool ou o driver de impressão HDI.
4. Quando o código de utilizador não é introduzido utilizando o driver de impressão PostScript 3, o driver universal PS3, a Web Printing Tool ou driver de impressão HDI.
5. Um trabalho da impressora ou ficheiro PDF é enviado de um computador host sem driver de impressão e impresso via LPR.
6. Um ficheiro PDF é impresso via ftp. A autenticação pessoal é realizada através da identificação do utilizador e a palavra-passe utilizadas para o início de sessão através de ftp. Contudo, a identificação do utilizador e a palavra-passe não estão encriptadas.

Níveis de autenticação e tipos dos trabalhos da impressora

Autenticação do Trabalho da Impressora	Simples (Todos)	Na totalidade
Trabalho da Impressora Tipo 1	C*1	C*1
Trabalho da Impressora Tipo 2	X	X
Trabalho da Impressora Tipo 3	A	B
Trabalho da Impressora Tipo 4	A	X
Trabalho da Impressora Tipo 5	A	X
Trabalho da Impressora Tipo 6	B	B

*1 Imprimir com autenticação por código de utilizador é classificado como B.

A: A impressão é possível independentemente da autenticação de utilizador.

B: A impressão é possível se a autenticação de utilizador for bem sucedida. Se a autenticação de utilizador falhar, o trabalho de impressão é apagado.

C: A impressão é possível se a autenticação do utilizador for bem sucedida e se o "Código de encriptação do controlador" do driver de impressão e do equipamento for o mesmo.

X: A impressão não é possível independentemente da autenticação de utilizador e o trabalho de impressão é apagado.

Nota

- Para mais informações sobre "Chave encript. driver: Grau de encriptação", consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".

Comando "authfree"

Se [Simples (Limitação)] estiver selecionado na autenticação do trabalho da impressora, pode utilizar o comando telnet authfree para especificar as excepções à autenticação do trabalho da impressora.

Para mais informações sobre o nome de utilizador e palavra-passe de início de sessão no telnet, pergunte ao administrador. Para detalhes sobre como iniciar sessão e usar telnet, consulte Ligação do Equipamento/Definições do Sistema.

Visualizar definições

```
msh> authfree
```

Se a exclusão de autenticação do trabalho de impressão não for especificado, não é possível visualizar o controlo de exclusão de autenticação.

Definições do endereço IPv4

```
msh> authfree "ID" range "start-address" "end-address"
```

Definições do endereço IPv6

```
msh> authfree "ID" range6 "start-address" "end-address"
```

Definições de máscara do endereço IPv6

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

Definições USB

```
msh> authfree usb [on|off]
```

Para excluir ligações USB da autenticação dos trabalhos da impressora, defina-as como "on". A predefinição é "off".

Inicialização do controlo de exclusão de autenticação

```
msh> authfree flush
```

Nota

- Nos ambientes IPv4 e IPv6, podem ser registados e selecionados até 5 intervalos de acesso.

Registo Automático no Livro de Endereços

As informações pessoais dos utilizadores que iniciam sessão através de autenticação no Windows ou LDAP são automaticamente registadas no livro de endereços. Quaisquer outras informações podem ser especificadas por cópia a partir de outros utilizadores registados.

Itens registados automaticamente no livro de endereços

- Nome de utilizador para início de sessão
- Palavra-passe para início de sessão
- N.º de registo
- Nome*1
- Nome visualizado*1
- Endereço de e-mail*2
- Proteger ficheiro(s) PermissõesUtiliz/Grupos*3

*1 Se não for possível obter esta informação, é registado o nome de utilizador de início de sessão neste campo.

*2 Se não for possível obter esta informação, o registo automático não funciona.

*3 Se [Defin transf dados p/programa auto livro endereços] for especificado em [Transferir dados], tem prioridade.

Nota

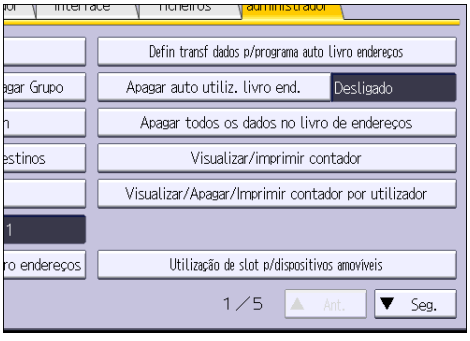
- Ao efetuar o registo automático, pode eliminar automaticamente contas de utilizador antigas se o volume de dados registados no livro de endereços tiver atingido o limite. Para mais informações, consulte Pág. 233 "Gerir o Livro de Endereços".

Defin transf dados p/programa auto livro endereços

As informações que não sejam registadas automaticamente no livro de endereços podem ser copiadas a partir de um utilizador já registado, ficando, em seguida, registadas.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**

4. **Prima [Defin transf dados p/programa auto livro endereços].**



5. **Prima [Transferir dados]**
6. **Utilize as teclas numéricas para introduzir o número de registo do livro de endereços a aplicar à definição especificada e, em seguida, prima [#].**
7. **Prima [OK].**
8. **Prima a tecla [Iniciar/Encerrar sessão].**

   É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Função de Bloqueio de Utilizadores

Se se introduzir várias vezes uma palavra-passe incorreta, a função de bloqueio de utilizador impede mais tentativas de início de sessão com o mesmo nome de utilizador de início de sessão. Mesmo que o utilizador bloqueado introduza a palavra-passe correta posteriormente, a autenticação falhará e o equipamento não poderá ser utilizado até que o período de bloqueio termine ou até que um administrador ou supervisor desative o bloqueio.

Para utilizar a função de bloqueio para autenticação de utilizador, o método de autenticação tem de estar definido como autenticação básica. Com outros métodos de autenticação, a função de bloqueio protege apenas as contas do supervisor e do administrador, não as contas dos utilizadores gerais.

Itens da definição de bloqueio

As definições da função de bloqueio podem ser efetuadas utilizando o Web Image Monitor.

Item de definição	Descrição	Valores da definição	Predefinição
Bloqueio	Especifique se ativa ou não a função de bloqueio.	• Ativo • Inativo	Inativo
Número de tentativas antes de bloquear	Especifique o número de tentativas de autenticação permitidas antes da aplicação do bloqueio.	1-10	5
Temporizador de bloqueio de conta	Especifique se pretende ou não cancelar o bloqueio após decorrido um período especificado.	• Ativo • Inativo	Inativo
Bloquear utilizador durante	Especifique o número de minutos após o qual o bloqueio é cancelado.	1-9.999 min.	60 min.

Privilégios para desbloqueio

Os administradores com privilégios de desbloqueio são os seguintes:

Utilizador bloqueado	Administrador de desbloqueio
Utilizador geral	Administrador de utilizadores
Administrador de utilizadores, administrador da rede, administrador de ficheiros, administrador do equipamento	Supervisor
Supervisor	Administrador do equipamento

Especificar a função de bloqueio de utilizadores

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Política de bloqueio de utilizador] sob "Segurança".**
4. **Defina "Bloqueio" para [Ativo].**
5. **No menu de lista, selecione o número de tentativas de início de sessão permitidas antes da aplicação do bloqueio.**
6. **Após o bloqueio, se pretender cancelar o mesmo após decorrido um determinado tempo, defina "Temporizador de bloqueio de conta" como [Ativo].**
7. **No campo "Bloquear utilizador durante", introduza o número de minutos até à desativação do bloqueio.**
8. **Clique em [OK].**

   Está definida a Política de bloqueio de utilizador.
9. **Encerre sessão.**

Cancelar o bloqueio da palavra-passe

1. **Inicie sessão como administrador de utilizadores a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Livro de endereços].**
3. **Selecione a conta do utilizador bloqueada.**
4. **Clique em [Introdução detalhada] e, em seguida, clique em [Alterar].**
5. **Defina "Bloqueio" como [Inativo] sob "Informações de autenticação".**
6. **Clique em [OK].**
7. **Encerre sessão.**

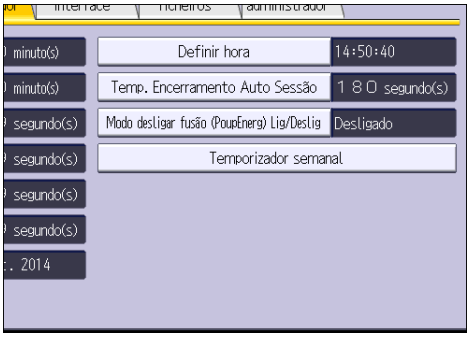
Nota

- Pode cancelar o bloqueio de palavra-passe do administrador e supervisor desligando a corrente e ligando-a novamente ou cancelando a definição em [Programar/Alterar administrador] sob [Configuração] no Web Image Monitor.

Encerramento Automático de Sessão

Depois de iniciar sessão, o equipamento encerra automaticamente a sessão se não utilizar o painel de controlo durante um determinado período de tempo. Esta função é chamada "Encerramento automático de sessão". Especifique o período de tempo que o equipamento deve aguardar antes de realizar o encerramento automático de sessão.

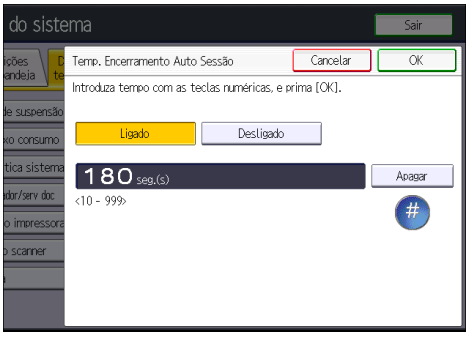
1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Defin. temporiz.].**
4. **Prima [Temp. Encerramento Auto Sessão].**



5. **Selecione [Ligado].**

   Se não pretender especificar [Temp. Encerramento Auto Sessão], selecione [Desligado].

6. **Introduza "10" a "999" (segundos) utilizando as teclas numéricas e, em seguida, prima [#].**



   Caso se engane, prima [Apagar].

7. **Prima [OK].**
8. **Prima a tecla [Iniciar/Encerrar sessão].**

   É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Nota

- Pode especificar as definições de encerramento automático de sessão para o Web Image Monitor em [Página web]. Para obter mais informações, consulte a Ajuda do Web Image Monitor.

Autenticação Utilizando um Dispositivo Externo

Se utilizar um dispositivo externo para efetuar autenticações, consulte o manual do dispositivo.

Para mais informações, contacte o seu consultor comercial.

3. Restringir a Utilização do Equipamento

Este capítulo explica como restringir a utilização do equipamento por parte do utilizador.

Restringir Uso da Lista de Destinos

O uso da lista de destinos pode ser restringido separadamente nas funções de scanner.

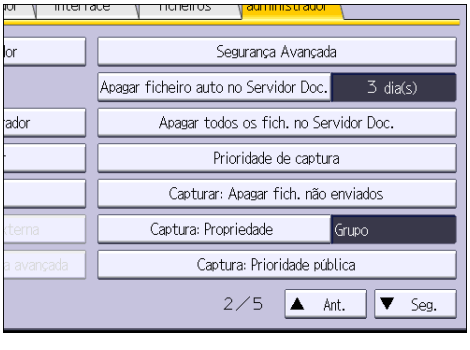
Restringir utilização de destinos

Pode proibir o envio de documentos digitalizados para endereços não registados no livro de endereços. Ao ativar esta opção, pode proibir os utilizadores de introduzirem manualmente o endereço de e-mail ou pastas de destino da parte.

Restringir adição de destinos utilizadores

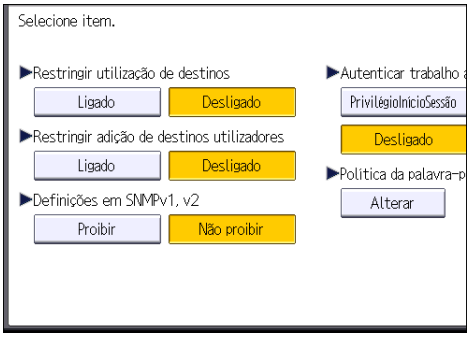
Utilizando [ProgDest], pode proibir que os endereços introduzidos manualmente para enviar documentos digitalizados sejam registados no livro de endereços. Além disso, com esta definição, apenas o administrador de utilizadores pode registar novos utilizadores no livro de endereços e alterar as palavras-passe e outras informações de utilizadores registados já existentes. Note também que, mesmo que defina estas funções como [Ligado], o utilizador registado como destino pode alterar a respetiva palavra-passe. Apenas o administrador de utilizadores pode alterar outros itens que não sejam palavras-passe.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Segurança Avançada].**



6. **Prima [▼Seg.].**

7. **Defina "Restringir utilização de destinos" ou "Restringir adição de destinos utilizadores" como [Ligado].**



Se definir "Restringir utilização de destinos" como [Ligado], "Restringir a adição de destinos utilizadores" não aparecerá.

8. **Prima [OK].**
9. **Prima a tecla [Iniciar/Encerrar sessão].**

É visualizada uma mensagem de confirmação. Se premir [Sim], a sessão é encerrada automaticamente.

Impedir Alterações às Definições dos Administradores

Limitar as definições que podem ser alteradas por cada administrador

As definições que podem ser efetuadas neste equipamento variam conforme o tipo de administrador, o que permite que a amplitude de operações que podem ser executadas seja partilhada entre os administradores.

Estão definidos os administradores seguintes para este equipamento:

- Administrador de utilizadores
- Administrador do equipamento
- Administrador de rede
- Administrador de ficheiros

Para mais informações sobre as definições que podem ser configuradas por cada administrador, consulte Pág. 269 "Lista de Privilégios de Operação para Definições".

Registe os administradores antes de utilizar o equipamento. Para instruções sobre como registar administradores, consulte Pág. 16 "Registar e alterar administradores".

Proibir utilizadores de efetuar alterações às definições

É possível proibir os utilizadores de efetuar alterações às definições dos administradores.

Selecione o item sob "Definições disponíveis" em "Gestão de autenticação do administrador" para impedir essas alterações.

Para mais infomações sobre os itens que podem ser selecionados em "Definições disponíveis", consulte Pág. 13 "Configurar a Autenticação dos Administradores".

Especificar a Função de Menu Protegido

A função de Menu protegido permite-lhe limitar a permissão dos utilizadores para aceder às definições no menu Ferramentas do Utilizador, exceto para as Definições do sistema. Esta definição pode ser utilizada independentemente da autenticação do utilizador. Para especificar a definição de Menu protegido, ative previamente a autenticação de administrador para o administrador do equipamento. Para mais informações sobre como definir a autenticação de administrador, consulte Pág. 13 "Configurar a Autenticação dos Administradores". Para obter uma lista das definições que os utilizadores podem especificar de acordo com o nível de proteção de menus, consulte Pág. 269 "Lista de Privilégios de Operação para Definições".

Se pretender ativar "Menu protegido", defina como [Nível 1] ou [Nível 2]. Selecione [Nível 2] para impor restrições mais fortes às permissões de acesso dos utilizadores às definições do equipamento.

Se pretender desativar "Menu protegido", defina como [Desligado].

Função de cópia

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Funções de copiador/servidor documentos].**
3. **Prima [Ferr. Administrador].**
4. **Prima [Menu protegido].**
5. **Selecione o nível de proteção do menu e, em seguida, prima [OK].**
6. **Encerre sessão.**

Função de impressora

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Funções de impressora].**
3. **Prima [Gestão de dados].**
4. **Prima [Menu protegido].**
5. **Selecione o nível de proteção do menu e, em seguida, prima [OK].**
6. **Encerre sessão.**

Função de scanner

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Funções de scanner].**

3. **Prima [Definições Iniciais].**
4. **Prima [Menu protegido].**
5. **Selecione o nível de proteção do menu e, em seguida, prima [OK].**
6. **Encerre sessão.**

Impedir utilizadores de registar/alterar programas

Ativar a definição Menu protegido permite impedir os utilizadores de registar ou alterar programas. Quando a definição está ativada, o administrador do equipamento é quem regista e altera programas.

Para mais informações sobre registar e alterar programas, consulte Convenient Functions.

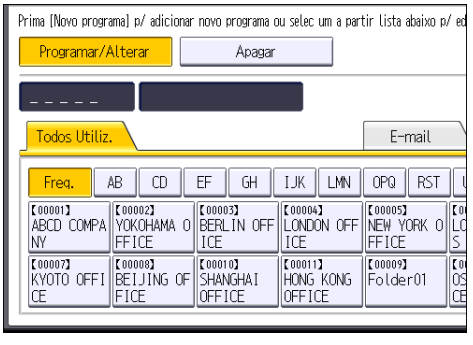
Limitar as Funções Disponíveis

Para impedir operações não autorizadas, pode especificar quem está autorizado a aceder a cada uma das funções do equipamento.

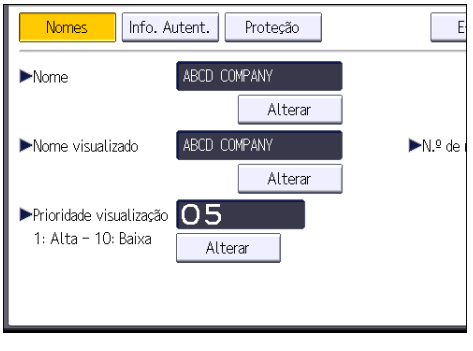
Especifique as funções disponíveis a utilizadores registados. Ao configurar esta definição, pode limitar as funções disponíveis aos utilizadores.

É possível estabelecer limites à utilização das funções de copiador, servidor de documentos, scanner, impressora e funções avançadas.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Gestão livro de endereços].**
3. **Selecione o utilizador.**

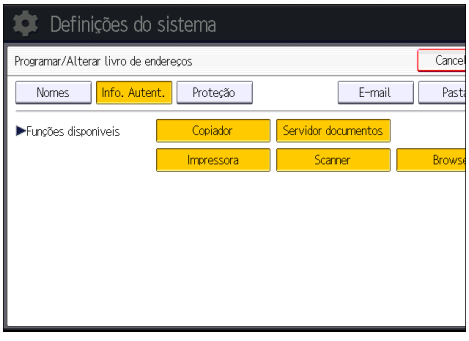


4. **Prima [Info. Autent.].**



5. **Prima [▼Seg.] duas vezes.**

6. **Em "Funções disponíveis", selecione as funções que pretende especificar.**

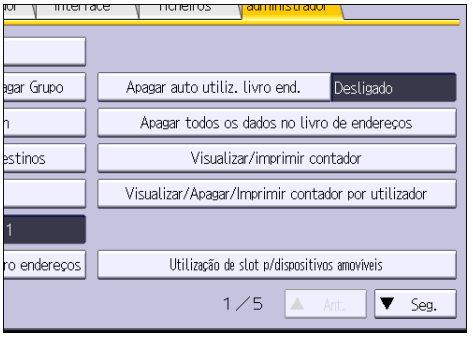


7. **Prima [OK].**
8. **Encerre sessão.**

Restringir o Acesso à Slot para Dispositivos de Armazenamento Amovível

Especifique no painel de controlo se permite ou não que os utilizadores utilizem as slots para dispositivos amovíveis. Com esta definição, pode restringir o armazenamento de ficheiros digitalizados num dispositivo de memória amovível. Além disso, com esta definição, pode restringir a impressão de ficheiros guardados num dispositivo de memória amovível.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [Utilização de slot p/dispositivos amovíveis].**



5. **Para restringir o armazenamento de ficheiros num dispositivo de memória amovível, prima [Proibir] sob "Guardar no dispositivo de memória".**
6. **Para restringir a impressão de ficheiros guardados num dispositivo de memória amovível, prima [Proibir] sob "Imprimir a partir de dispositivo de memória".**
7. **Prima [OK].**
8. **Encerre sessão.**

Nota

- Se selecionar [Proibir] em "Guardar no dispositivo de memória", o botão de [Guardar no disposit. mem.] não aparece no ecrã de Guardar fich. da função de scanner.
- Se selecionar [Proibir] em "Imprimir a partir de dispositivo de memória",o botão [Imprimir a partir de dispositivo de memória] não aparece no ecrã inicial da função de impressora.

4. Prevenir Contra Fugas de Informação a partir de Equipamentos

Este capítulo explica como proteger informações guardadas na memória do equipamento ou no disco rígido.

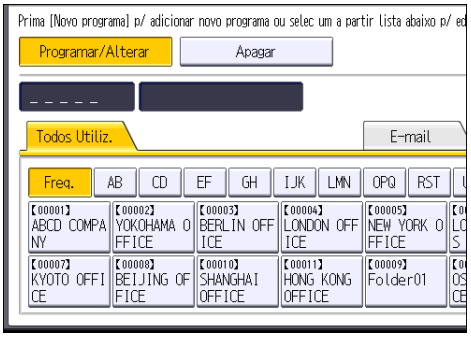
Proteger o Livro de Endereços

Pode especificar a quem é permitido o acesso aos dados no livro de endereços. Para proteger os dados contra utilizadores não autorizados, pode também encriptar os dados no livro de endereços.

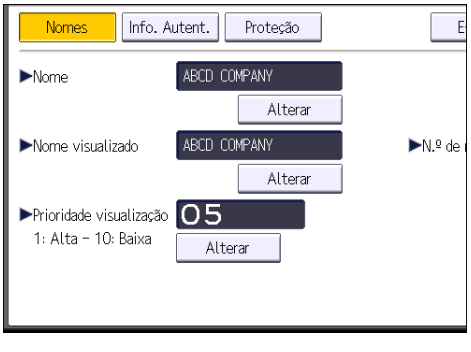
Especificar permissões de acesso ao livro de endereços

As permissões de acesso podem ser configuradas pelos utilizadores registados no livro de endereços, utilizadores com privilégios de controlo total e pelo administrador de utilizadores.

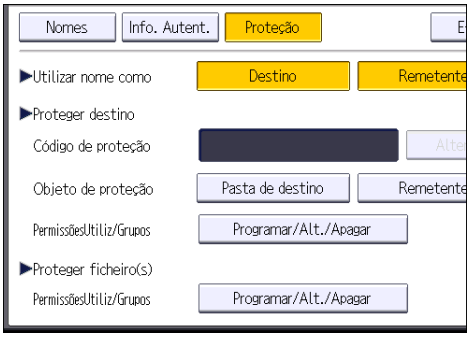
1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Gestão livro de endereços].**
3. **Selecione o utilizador cuja permissão de acesso pretende alterar.**



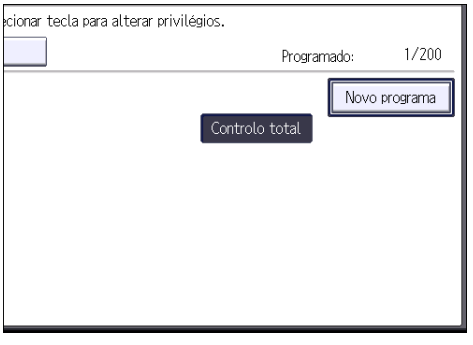
4. **Prima [Proteção].**



5. **Prima [Programar/Alt./Apagar] para "PermissõesUtiliz/Grupos", em "Proteger destino".**



6. **Prima [Novo programa].**



7. **Selecione os utilizadores ou grupos aos quais pretende aplicar permissões de acesso.**

   Pode selecionar vários utilizadores.

   Se premir [Todos os Utilizadores], pode selecionar todos os utilizadores.

8. **Prima [Sair].**
9. **Selecione o utilizador a quem pretende atribuir permissões de acesso, especificando depois a permissão.**

   Selecione uma das seguintes opções [Só de leitura], [Editar], [Editar/ Apagar] ou [Controlo total].

10. **Prima [Sair].**
11. **Prima [OK].**
12. **Encerre sessão.**

Nota

- As permissões de acesso "Editar", "Editar/ Apagar" e "Controlo total" permitem aos utilizadores executar operações que podem resultar em perda ou alteração de informações delicadas. Recomendamos que apenas se atribua a permissão "Só de leitura" à generalidade dos utilizadores.

Encriptar dados no livro de endereços

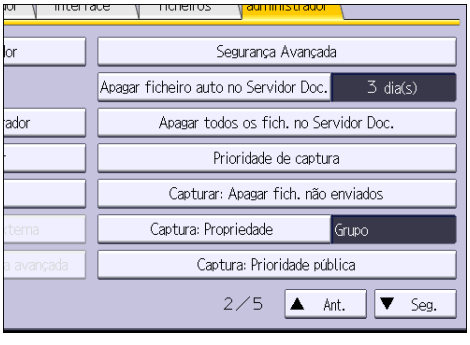
Importante

- **O equipamento não pode ser utilizado durante a encriptação.**

O tempo que demora a encriptar os dados do livro de endereços depende do número de utilizadores registados.

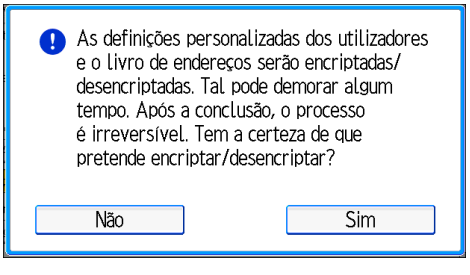
Encriptar os dados do livro de endereços pode demorar mais tempo.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Segurança Avançada].**



6. **Prima [Ligado] para "Encriptar defin. personaliz. utiliz.+livro endereços".**
7. **Prima [Alterar] para "Código de encriptação".**
8. **Introduza o código de encriptação e, em seguida, prima [OK].**

   Introduza o código de encriptação utilizando até 32 carateres alfanuméricos.
9. **Prima [Encriptar/ Desencriptar].**
10. **Prima [Sim].**


As definições personalizadas dos utilizadores e o livro de endereços serão encriptadas/ desencriptadas. Tal pode demorar algum tempo. Após a conclusão, o processo é irreversível. Tem a certeza de que pretende encriptar/desencriptar?
Não
Sim

Não desligue a alimentação principal durante a encriptação, pois tal poderá danificar os dados.

Se premir [Parar] durante a encriptação, os dados não são encriptados.

Se premir [Parar] durante a desencriptação, os dados não são desencriptados.

Normalmente, assim que a encriptação estiver concluída, é visualizada a mensagem "Encriptação/Desencriptação terminada com sucesso. Prima [Sair].".

11. **Prima [Sair].**
12. **Prima [OK].**
13. **Encerre sessão.**

Nota

- Se registar utilizadores adicionais depois de encriptar os dados no livro de endereços, os dados desses utilizadores também são encriptados.
- O backup dos dados do livro de endereços guardados no SD card é encriptado. Para mais informações sobre como fazer uma cópia de segurança e repor o livro de endereços utilizando um SD card, consulte Connecting the Machine/System Settings.

Encriptar Dados no Equipamento

⚠CUIDADO

- Mantenha os SD cards ou dispositivos de memória flash USB fora do alcance das crianças. Se uma criança engolir acidentalmente um SD card ou um dispositivo de memória flash USB, consulte imediatamente um médico.

Mesmo que o dispositivo de memória ou o disco rígido seja roubado, é possível evitar a fuga de dados encriptando os dados no equipamento, como por exemplo o livro de endereços, dados de autenticação e ficheiros.

Todos os dados guardados no equipamento depois de a encriptação ser ativada serão encriptados.

Também pode optar por encriptar ou apagar os dados já guardados no equipamento.

O algoritmo de encriptação é AES-256.

Dados que são encriptados

Esta função encripta dados guardados na NVRAM (memória que permanece mesmo depois do equipamento ser desligado) e no disco rígido do equipamento.

Os dados seguintes são encriptados:

NVRAM

- Informações de definições do sistema
- Informações de definição do interface de rede
- Informações de código de utilizador
- Informações de contador

Disco rígido

- Livro de endereços
- Programa/registo de aplicações de Embedded Software Architecture
- Registos (registo de trabalhos/registo de acessos/registo ecológico)
- E-mail enviado/recebido
- Tipos de letra registados
- Trabalhos em spool
- Miniaturas de documentos guardados
- Documentos reencaminhados para o servidor de captura
- Documentos guardados
- Carimbos registados

Tipo de encriptação

Especifique se pretende encriptar os dados existentes e guardá-los no disco rígido ou eliminá-los (formatar). A encriptação é demorada se houver uma grande quantidade de dados a guardar. Os dados NVRAM não serão apagados (inicializados).

Definição	Dados guardados	Dados a serem inicializados	Tempo necessário
Apenas dados sistema fich	• Livro de endereços • Programa/registo de aplicações de Embedded Software Architecture • Registos (registo de trabalhos/registo de acessos/registo ecológico) • E-mail enviado/ recebido • Tipos de letra registados • Trabalhos em spool • Miniaturas de documentos guardados • Documentos reencaminhados para o servidor de captura	• Documentos guardados (documentos guardados no servidor de documentos e ficheiros de impressão bloqueada / ficheiros de impressão de teste / ficheiros de impressão guardada / ficheiros de impressão retida) • Carimbos registados	Aprox. 2 horas e 30 minutos
Todos os dados	Todos os dados: Dados a guardar e dados a não guardar quando é especificado [Apenas dados sistema fich]	Nenhum	Aprox. 6 horas e 15 minutos
Formatar todos os dados	Nenhum	Todos os dados: Dados a guardar e dados a não guardar quando é especificado [Apenas dados sistema fich]	Vários minutos

Notas sobre a ativação das definições de encriptação

- Se utilizar a aplicação Embedded Software Architecture ou App2Me, certifique-se de que especifica [Apenas dados sistema fich] ou [Todos os dados].
- Tenha em atenção que as definições do equipamento não serão repostas para as suas predefinições mesmo que seja especificado [Formatar todos os dados], [Apenas dados sistema fich] ou [Todos os dados].

Repor dados

- Para transferir dados para um novo equipamento, reponha os dados encriptados. Peça mais informações à assistência técnica.
- O código de encriptação utilizado na encriptação dos dados é necessário para repor os dados.
- Pode especificar se pretende imprimir o código de encriptação ou guardá-lo num SD card.
- Pode alterar a chave de encriptação posteriormente.

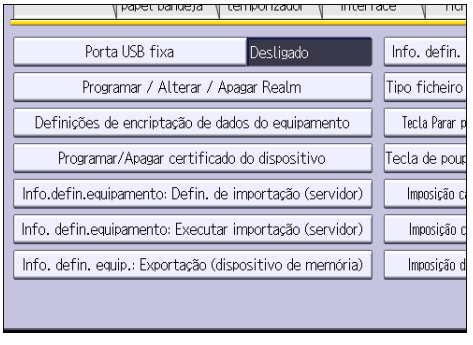
Ativar as definições de encriptação

Importante

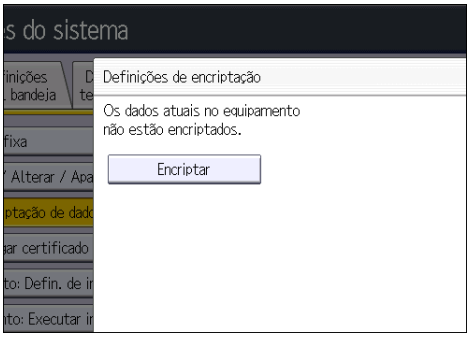
- **Não é possível utilizar o equipamento durante a encriptação de dados.**
- **Assim que o processo de encriptação iniciar, não é possível pará-lo. Certifique-se de que o equipamento não é desligado enquanto estiver a decorrer o processo de encriptação. Se o equipamento for desligado enquanto estiver a decorrer a encriptação, o disco rígido ficará danificado e os dados contidos nele ficarão inutilizados.**
- **É necessário o código de encriptação para a recuperação de dados se o equipamento avariar. Certifique-se de que guarda a chave de encriptação em segurança para recuperar dados da cópia de segurança.**
- **A encriptação começa após ter concluído o procedimento do painel de controlo e ter reiniciado o equipamento, desligando e ligando a alimentação principal. Se as funções de Apagar toda a memória e de encriptação estiverem especificadas, a encriptação tem início depois de os dados guardados no disco rígido terem sido substituídos e o equipamento ter sido reiniciado, desligando e ligando a alimentação principal.**
- **Se utilizar Apagar toda a memória e encriptação em simultâneo, e se selecionar substituir 3 vezes para "Números aleatórios", o processo poderá demorar até 11 horas e 30 minutos. A reencriptação a partir de um estado já encriptado demora o mesmo tempo.**
- **A função "Apagar toda a memória" também apaga todas as definições de segurança do equipamento, fazendo com que não seja possível fazer a gestão do equipamento e de utilizadores. Certifique-se de que os utilizadores não guardam quaisquer dados no equipamento após "Apagar toda a memória" ter terminado.**

- Reiniciar o equipamento será mais rápido se não existirem dados a transferir para o disco rígido e se não estiver definida nenhuma encriptação para [Formatar todos os dados], mesmo que todos os dados no disco rígido sejam formatados. Antes de efetuar a encriptação, recomendamos que faça cópias de segurança de dados importantes, como o livro de endereços e todos os dados guardados no servidor de documentos.

1. Inicie sessão como administrador do equipamento no painel de controlo.
2. Prima [Definições do sistema].
3. Prima [Ferr. Administrador].
4. Prima [▼Seg.] 3 vezes.
5. Prima [Definições de encriptação de dados do equipamento].


Porta USB fixa
Desligado
Info. defin.
Programar / Alterar / Apagar Realm
Tipo ficheiro
Definições de encriptação de dados do equipamento
Programar/Apagar certificado do dispositivo
Info.defin.equipamento: Defin. de importação (servidor)
Info. defin.equipamento: Executar importação (servidor)
Info. defin. equip.: Exportação (dispositivo de memória)

6. Prima [Encriptar].



7. Selecione os dados a serem transferidos para o disco rígido e a não serem apagados.

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Apenas dados sistema fich]. Para apagar todos os dados, selecione [Formatar todos os dados].

8. Especifique o modo como será feita a cópia de segurança da chave de encriptação.

   Se tiver selecionado [Guardar em SD], insira um SD card na slot de dispositivo de memória amovível, localizada na lateral do painel de controlo e prima [OK] para fazer uma cópia de segurança da chave de encriptação do equipamento.

   Para mais informações sobre como manusear e inserir o SD card, consulte Getting Started.

Se tiver selecionado [Impr. em papel], prima a tecla [Iniciar] e imprima a chave de encriptação do equipamento.

9. **Prima [OK].**
10. **Prima [Sair].**
11. **Prima [Sair].**
12. **Encerre sessão.**
13. **Desligue o interruptor de alimentação e, em seguida, volte a ligá-lo.**

    O equipamento começará a converter os dados na memória após ligar o equipamento. Aguarde até ser visualizada a mensagem "Conversão de memória concluída. Desligue o equipamento." e, em seguida, volte a desligar os interruptores de corrente principais.

    Para mais informações sobre como desligar o equipamento, consulte Getting Started.

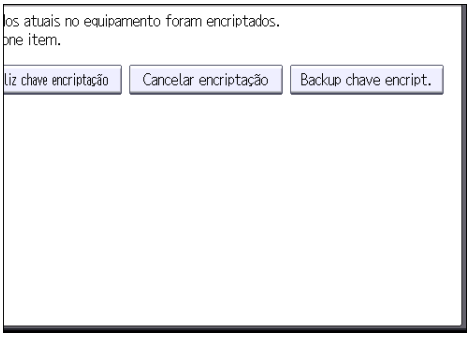
Efetuar cópia de segurança da chave de encriptação

É possível fazer uma cópia de segurança da chave de encriptção sem alterar a definição de encriptação.

Importante

- **É necessário o código de encriptação para a recuperação de dados se o equipamento avariar. Certifique-se de que guarda a chave de encriptação em segurança para recuperar dados da cópia de segurança.**

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Prima [Definições de encriptação de dados do equipamento].**
6. **Prima [Backup chave encript.].**



7. **Especifique o modo como será feita a cópia de segurança da chave de encriptação.**

   Se tiver selecionado [Guardar em SD], insira um SD card na slot de dispositivo de memória amovível, localizada na lateral do painel de controlo e prima [OK]. Quando a criação da cópia de segurança da chave de encriptação de dados do equipamento estiver concluída, prima [Sair].

   Para mais informações sobre como manusear e inserir o SD card, consulte Getting Started.

   Se tiver selecionado [Impr. em papel], prima a tecla [Iniciar] e imprima a chave de encriptação do equipamento.

8. **Prima [Sair].**
9. **Encerre sessão.**

Atualizar a chave de encriptação

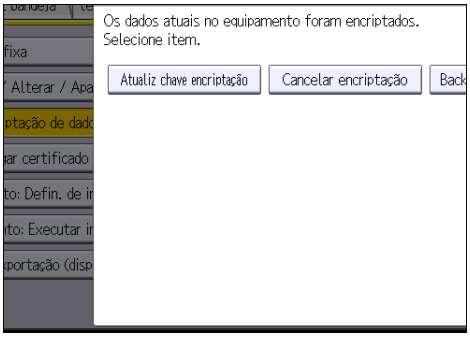
Pode atualizar a chave de encriptação. Aplicar a nova chave de encriptação demora o mesmo tempo que a encriptação inicial. É possível proceder a atualizações se o equipamento estiver a funcionar normalmente.

Importante

- O equipamento não pode ser utilizado enquanto a chave de encriptação estiver a ser atualizada.
- O código de encriptação é necessário para recuperação se o equipamento avariar. Certifique-se de que guarda a chave de encriptação em segurança para recuperar dados da cópia de segurança.
- Quando a chave de encriptação é atualizada, a encriptação é efetuada utilizando a nova chave. Depois de concluir o procedimento no painel de controlo do equipamento, desligue o equipamento e reinicie-o para ativar as novas definições. Reiniciar o equipamento pode processar-se de forma lenta se existirem dados que precisem de ser transferidos para o disco rígido.
- Depois de começar, a atualização da chave de encriptação não pode ser interrompida. Certifique-se de que o equipamento não é desligado enquanto estiver a decorrer o processo de encriptação. Se o equipamento for desligado enquanto estiver a decorrer a encriptação, o disco rígido ficará danificado e os dados contidos nele ficarão inutilizados.
- Se a atualização da chave de encriptação não for concluída, a chave de encriptação criada não será válida.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Prima [Definições de encriptação de dados do equipamento].**

6. **Prima [Atualiz chave encriptação].**



7. **Selecione os dados a serem transferidos para o disco rígido e a não serem apagados.**

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Apenas dados sistema fich]. Para apagar todos os dados, selecione [Formatar todos os dados].

8. **Especifique o modo como será feita a cópia de segurança da chave de encriptação.**

   Se tiver selecionado [Guardar em SD], insira um SD card na slot de dispositivo de memória amovível, localizada na lateral do painel de controlo e prima [OK] para fazer uma cópia de segurança da chave de encriptação do equipamento.

   Para mais informações sobre como manusear e inserir o SD card, consulte Getting Started.

   Se tiver selecionado [Impr. em papel], prima a tecla [Iniciar] e imprima a chave de encriptação do equipamento.

9. **Prima [OK].**
10. **Prima [Sair].**
11. **Prima [Sair].**
12. **Encerre sessão.**
13. **Desligue o interruptor de alimentação e, em seguida, volte a ligá-lo.**

    O equipamento começará a converter os dados na memória após ligar o equipamento. Aguarde até ser visualizada a mensagem "Conversão de memória concluída. Desligue o equipamento." e, em seguida, volte a desligar os interruptores de corrente principais.

    Para mais informações sobre como desligar o equipamento, consulte Getting Started.

Cancelar a encriptação de dados

Utilize o procedimento que se segue para cancelar as definições de encriptação quando esta já não for necessária. Ativar e desativar as definições de encriptação demora o mesmo tempo.

Importante

- **Não é possível utilizar o equipamento durante o cancelamento da encriptação de dados.**

- Depois de concluir este procedimento no painel de controlo do equipamento, desligue o equipamento e reinicie-o para ativar as novas definições. Reiniciar o equipamento pode processar-se de forma lenta se existirem dados que precisem de ser transferidos para o disco rígido.
- Assim que o cancelamento da encriptação dos dados é iniciado, não é possível interrompê-lo. Certifique-se de que o equipamento não é desligado enquanto estiver a decorrer o processo de encriptação. Se o equipamento for desligado enquanto estiver a decorrer a encriptação, o disco rígido ficará danificado e os dados contidos nele ficarão inutilizados.
- Quando eliminar um equipamento, apague completamente a memória. Para mais informações sobre como apagar toda a memória, consulte Pág. 85 "Apagar Dados no Equipamento".

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Prima [Definições de encriptação de dados do equipamento].**
6. **Prima [Cancelar encriptação].**
7. **Selecione os dados a serem transferidos para o disco rígido e a não serem apagados.**

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Apenas dados sistema fich]. Para apagar todos os dados, selecione [Formatar todos os dados].
8. **Prima [OK].**
9. **Prima [Sair].**
10. **Prima [Sair].**
11. **Encerre sessão.**
12. **Desligue o interruptor de alimentação e, em seguida, volte a ligá-lo.**

    Para mais informações sobre como desligar o equipamento, consulte Getting Started.

Apagar Dados no Equipamento

É possível evitar a fuga de dados através da substituição dos dados guardados no equipamento.

Há os seguintes dois tipos de substituição:

Apagar auto memória

Os dados guardados temporariamente no disco rígido do equipamento para copiar ou imprimir são apagados automaticamente. Para obter detalhes, consulte Pág. 85 "Apagar auto memória".

Apagar toda a memória

Todos os dados guardados no disco rígido do equipamento são apagados por substituição. As definições do dispositivo guardadas na memória do equipamento são inicializadas. Execute esta função para apagar todos os dados e definições quando mudar o equipamento de local ou proceder à sua deposição. Para obter detalhes, consulte Pág. 89 "Apagar toda a memória".

Apagar auto memória

Um documento digitalizado no modo de copiador ou scanner ou os dados de impressão enviados a partir de um driver de impressão são temporariamente guardados no disco rígido do equipamento. Mesmo depois de terminado o trabalho, mantêm-se no disco rígido como dados temporários. A função Apagar memória auto apaga os dados temporários no disco rígido substituindo-os.

A substituição começa automaticamente assim que o trabalho tiver terminado.

As funções de impressora e copiador têm prioridade sobre a função de Apagar auto memória. Se estiver em curso um trabalho de cópia ou impressão, a substituição só será realizada após a conclusão do trabalho.

Tipos de dados que podem ou não ser substituídos pela função Apagar auto memória

Dados substituídos pela função Apagar auto memória

Copiador

- Trabalhos de cópia

Impressora

- Trabalhos de impressão
- Trabalhos de Impressão de teste/Impressão bloqueada/Reter impressão/Impressão guardada

  Um trabalho de Impressão de teste/Impressão bloqueada/Reter impressão apenas pode ser substituído após ter sido executado. Um trabalho de Impressão guardada é substituído após ter sido apagado.

- Trabalhos de impressão em spool

Scanner

- Ficheiros digitalizados enviados por e-mail
- Ficheiros enviados por Scan to Folder
- Documentos enviados utilizando o Web Image Monitor

Servidor de documentos

- Documentos guardados pelo utilizador no servidor de documentos utilizando as funções de copiador, impressora ou scanner

  Um documento guardado só pode ser substituído depois de ter sido impresso ou apagado do Servidor de documentos.

Outros

- Informação registada no livro de endereços

  Os dados guardados no livro de endereços só podem ser substituídos depois de terem sido alterados ou apagados.

- Aplicações que utilizam Embedded Software Architecture

  Os dados do programa Embedded Software Architecture só podem ser substituídos depois de terem sido apagados.

Dados não substituídos pela função Apagar auto memória

- Contadores sob cada código de utilizador

Métodos de substituição

Pode selecionar um dos seguintes métodos de substituição:

- NSA

  Os dados temporários são substituídos duas vezes por números aleatórios e uma vez por zeros.

- DoD

  Cada dado é substituído por um número aleatório, seguido do respetivo complemento e ainda por outro número aleatório, sendo finalmente verificado.

- Números aleatórios

  Os dados temporários são substituídos várias vezes por números aleatórios. O número de substituições pode ser selecionado de 1 a 9.

Nota

- O método predefinido para substituição é "Números aleatórios" e o número predefinido de substituições é 3.
- NSA significa "National Security Agency", EUA

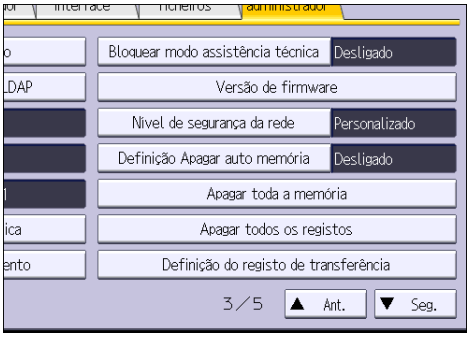
- DoD significa "Department of Defense", E.U.A.

Utilizar Apagar Auto Memória

Importante

- Quando Apagar memória auto estiver definido como [Ligado], os dados temporários que ficaram no disco rígido quando Apagar memória auto estava [Desligado] podem não ser substituídos.
- Se o interruptor de alimentação principal for desligado antes de concluída a operação de Apagar auto memória, a substituição será interrompida e os dados permanecerão no disco rígido.
- Não pare o processo de substituição a meio. Se o fizer, pode danificar o disco rígido.
- Se o interruptor de alimentação principal for desligado antes da função Apagar memória auto ter terminado, a substituição continuará assim que o interruptor de alimentação principal for novamente ligado.
- Se ocorrer um erro antes de a substituição ter sido concluída, desligue a alimentação. Volte a ligá-la e, em seguida, repita a partir do passo 1.
- O equipamento apenas entra em modo de suspensão após terminar a substituição.

1. Inicie sessão como administrador do equipamento no painel de controlo.
2. Prima [Definições do sistema].
3. Prima [Ferr. Administrador].
4. Prima [▼Seg.] duas vezes.
5. Prima [Definição Apagar auto memória].



6. Prima [Ligado].
7. Selecione o método de substituição que pretende utilizar.

   Se selecionar [NSA] ou [DoD], avance para o passo 10.

   Se selecionar [Números aleatórios], avance para o passo 8.
8. Prima [Alterar].

9. **Introduza o número de vezes que pretende efetuar a substituição utilizando as teclas numéricas e, em seguida, prima [#].**
10. **Prima [OK].**

    A opção Apagar auto memória fica definida.
11. **Encerre sessão.**

Nota

- Se ativar a substituição e a encriptação de dados, os dados da substituição também serão encriptados.

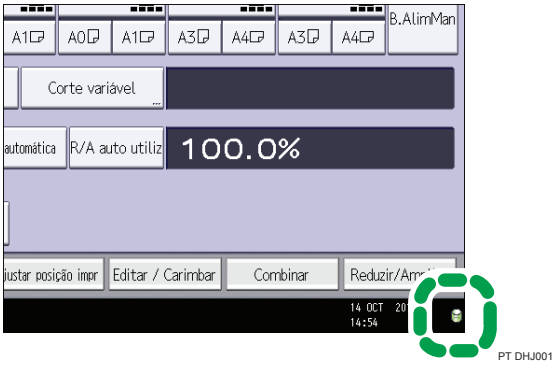
Cancelar a função de apagar a memória automaticamente

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] duas vezes.**
5. **Prima [Definição Apagar auto memória].**
6. **Prima [Desligado].**
7. **Prima [OK].**

   A opção Apagar auto memória fica desativada.
8. **Encerre sessão.**

Ícone de substituição

Quando a opção Apagar auto memória está ativada, o ícone Substituir dados será visualizado no canto inferior direito do visor do seu equipamento.



Ícone	Nome do ícone	Explicação
	Com dados	Este ícone acende quando existem dados temporários para eliminação e fica intermitente durante o processo.
	Sem dados	Este ícone acende quando não existem dados temporários a serem substituídos.

Importante

- **O ícone Substituir dados indicará "Sem dados" quando houver um trabalho de impressão de teste/impressão bloqueada/impressão retida/impressão guardada.**

Nota

- Se o ícone Substituir Dados não for visualizado, verifique primeiro se Apagar Auto Memória está definido como [Desligado]. Se o ícone não for visualizado mesmo que Apagar Auto Memória esteja [Ligado], contacte a assistência técnica.
- Se o equipamento entrar em modo de poupança de energia durante a substituição, prima a tecla [Poupança de energia] para reativar o visor e verificar o ícone.
- Se o ícone Substituir dados continuar "Com dados" quando não existirem dados a serem substituídos, desligue a alimentação principal do equipamento. Ligue-o novamente e veja se o ícone muda para "Sem dados". Se não mudar, contacte o consultor comercial ou a assistência técnica.

Apagar toda a memória

Substitua e apague todos os dados guardados no disco rígido quando mudar o equipamento de local ou proceder à sua deposição. As definições do dispositivo guardadas na memória do equipamento são inicializadas.

Para mais informações sobre a utilização do equipamento depois de executar a função Apagar toda a memória, contacte o seu consultor comercial.

Importante

- **Se o interruptor de alimentação principal for desligado antes de ter sido concluída a operação da função "Apagar toda a memória", a substituição será interrompida e os dados permanecerão no disco rígido.**
- **Não pare o processo de substituição a meio. Se o fizer, pode danificar o disco rígido.**
- **Recomendamos que, antes de apagar o disco rígido, utilize o Device Manager NX para fazer backup do livro de endereços. Também é possível fazer uma cópia de segurança do livro de endereços utilizando o Web Image Monitor. Para obter mais informações, consulte a Ajuda do Device Manager NX ou a Ajuda do Web Image Monitor.**

- **A única operação possível durante o processo "Apagar toda a memória" é colocar em pausa. Se "Números aleatórios" estiver selecionado e a substituição de dados estiver definida como 3 vezes, o processo "Apagar toda a memória" demora até 5 horas e 15 minutos.**
- **A função "Apagar toda a memória" também apaga todas as definições de segurança do equipamento, fazendo com que não seja possível fazer a gestão do equipamento e de utilizadores. Certifique-se de que os utilizadores não guardam quaisquer dados no equipamento após "Apagar toda a memória" ter terminado.**

Tipos de dados que podem ser substituídos por Apagar toda a memória

Copiador

- Trabalhos de cópia

Impressora

- Trabalhos de impressão
- Trabalhos de Impressão de teste/Impressão bloqueada/Reter impressão/Impressão guardada
- Trabalhos de impressão em spool

Scanner

- Ficheiros digitalizados enviados por e-mail
- Ficheiros enviados por Scan to Folder
- Documentos enviados utilizando o Web Image Monitor

Servidor de documentos

- Documentos guardados pelo utilizador no servidor de documentos utilizando as funções de copiador, impressora ou scanner

Outros

- Informação registada no livro de endereços
- Contadores sob cada código de utilizador
- Aplicações que utilizam ESA (Embedded Software Architecture)

Definições do sistema ou outras definições relacionadas com o dispositivo são inicializadas.

Métodos de eliminação

Pode selecionar um dos seguintes métodos de eliminação:

- NSA

  Os dados são substituídos duas vezes por números aleatórios e uma vez por zeros.
- DoD

Os dados são substituídos por um número aleatório, seguido do respetivo complemento e ainda por outro número aleatório, sendo verificados no fim.

- Números aleatórios

  Os dados são substituídos várias vezes por números aleatórios. O número de substituições pode ser selecionado de 1 a 9.

- BSI/VSITR

  Os dados são substituídos 7 vezes com os seguintes padrões: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.

- Eliminação segura

  Os dados são substituídos utilizando um algoritmo que está incorporado na unidade de disco rígido.

- Formatar

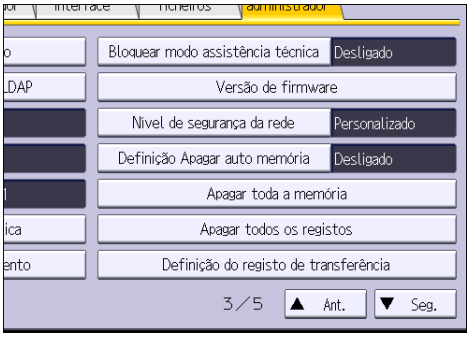
  O disco rígido está formatado. Os dados não são substituídos.

Nota

- O método predefinido para a eliminação é"Números aleatórios" e o número predefinido de substituições é 3.
- NSA significa "National Security Agency", EUA
- DoD significa "Department of Defense", E.U.A.

Utilizar Apagar toda a memória

1. **Desligue os cabos de comunicação ligados ao equipamento.**
2. **Inicie sessão como administrador do equipamento no painel de controlo.**
3. **Prima [Definições do sistema].**
4. **Prima [Ferr. Administrador].**
5. **Prima [▼Seg.] duas vezes.**
6. **Prima [Apagar toda a memória].**

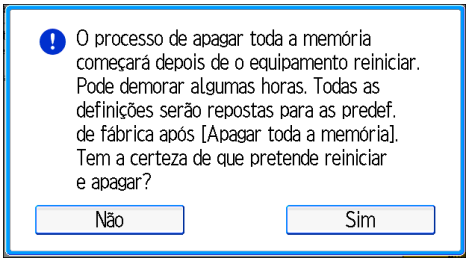


7. **Selecione o método de eliminação.**

   Se selecionar [NSA], [DoD], [BSI/VSITR], [Eliminação segura] ou [Formatar], avance para o passo 10.

   Se selecionar [Números aleatórios], avance para o passo 8.

8. **Prima [Alterar].**
9. **Introduza o número de vezes que pretende efetuar a substituição utilizando as teclas numéricas e, em seguida, prima [#].**
10. **Prima [Apagar].**
11. **Prima [Sim].**


O processo de apagar toda a memória começará depois de o equipamento reiniciar. Pode demorar algumas horas. Todas as definições serão repostas para as predef. de fábrica após [Apagar toda a memória]. Tem a certeza de que pretende reiniciar e apagar?
Não
Sim

12. **Quando a eliminação tiver sido concluída, prima [Sair] e desligue a alimentação.**

    Para mais informações sobre como desligar o equipamento, consulte Getting Started.

Nota

- Se o interruptor de alimentação principal for desligado antes de ter sido concluída a operação de "Apagar toda a memória", a substituição recomeçará assim que o interruptor de alimentação principal seja novamente ligado.
- Se ocorrer um erro antes de a substituição ter sido concluída, desligue a alimentação. Volte a ligar a alimentação e repita o procedimento a partir do passo 2.

Suspender a função Apagar toda a memória

Para desligar a alimentação elétrica do equipamento enquanto Apagar toda a memória está ativado, suspenda em primeiro lugar Apagar toda a memória. Apagar toda a memória será retomado quando voltar a ligar a alimentação elétrica do equipamento.

Importante

- **Se [Eliminação segura] ou [Formatar] tiver sido selecionado, não é possível suspender o processo.**
- **Apagar toda a memória não pode ser cancelado.**

1. **Prima [Suspender] enquanto Apagar toda a memória estiver em curso.**
2. **Prima [Sim].**

   Apagar toda a memória fica suspenso.

3. **Desligue a alimentação principal.**

   Para mais informações sobre como desligar o equipamento, consulte Getting Started.

5. Segurança de Rede Avançada

Este capítulo descreve as funções para aumentar a segurança quando o equipamento está ligado à rede.

Controlo de Acesso

O equipamento pode controlar o acesso por TCP/IP.

É possível limitar os endereços IP a partir dos quais se acede especificando um intervalo do controlo de acesso.

Por exemplo, se especificar um intervalo do controlo de acesso como [192.168.15.16]-[192.168.15.20], os endereços do PC cliente a partir dos quais o acesso é possível situar-se-ão entre [192.168.15.16] e [192.168.15.20].

Importante

- **Utilizando o controlo de acesso, é possível limitar os acessos de LPR, RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, WSD (Dispositivo), WSD (Impressora), IPP, DIPRINT ou Web Image Monitor. Não é possível limitar o acesso de telnet ou Device Manager NX quando SNMPv1 for usado para monitorização.**

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Controlo de acesso] sob "Segurança".**
4. **Para especificar o endereço IPv4, introduza um endereço IP que tenha acesso ao equipamento, em "Intervalo de controlo de acesso".**

   Para especificar o endereço IPv6, introduza um endereço IP com acesso ao equipamento em "Intervalo" sob "Intervalo de controlo de acesso" ou introduza um endereço IP em "Máscara" e especifique o "Comprimento de máscara".
5. **Clique em [OK].**
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Ativar e Desativar Protocolos

Especifique se pretende ativar ou desativar a função para cada protocolo. Ao efetuar esta definição, pode especificar quais os protocolos disponíveis, prevenindo assim o acesso não autorizado pela rede. As definições de rede podem ser especificadas no painel de controlo ou através do Web Image Monitor, telnet, Device Manager NX ou Remote Communication Gate S.

Protocolo	Porta	Método de definição	Quando desativado
IPv4	-	• Painel de controlo • Web Image Monitor • telnet	Nenhuma aplicação que opere através de IPv4 pode ser utilizada. IPv4 não pode ser desativado no Web Image Monitor quando utilizar a transmissão IPv4.
IPv6	-	• Painel de controlo • Web Image Monitor • telnet	Todas as aplicações que operem através de IPv6 não podem ser utilizadas.
IPsec	-	• Painel de controlo • Web Image Monitor • telnet	A transmissão encriptada utilizando IPsec é desativada.
FTP	TCP:21	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem FTP não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controlo utilizando "Restringir visualiz. informações utilizador".
ssh/sftp	TCP:22	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem sftp não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controlo utilizando "Restringir visualiz. informações utilizador".
telnet	TCP:23	• Web Image Monitor • Device Manager NX	Os comandos que utilizam telnet são desativados.

Protocolo	Porta	Método de definição	Quando desativado
SMTP	TCP:25 (variável)	• Painel de controlo • Web Image Monitor • Device Manager NX • Remote Communication Gate S	Não é possível utilizar a função de notificação por e-mail que requer a receção SMTP.
HTTP	TCP:80	• Web Image Monitor • telnet	As funções que requerem HTTP não podem ser utilizadas. Não é possível imprimir utilizando IPP na porta 80.
HTTPS	TCP:443	• Web Image Monitor • telnet	As funções que necessitam de HTTPS não podem ser utilizadas. Não é possível utilizar @Remote. Também pode efetuar definições para exigir transmissão SSL utilizando o painel de controlo ou o Web Image Monitor.
SMB	TCP:139	• Painel de controlo • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções de impressão SMB não podem ser utilizadas.
NBT	UDP:137 UDP:138	• telnet	As funções de impressão SMB através de TCP/IP, bem como as funções designadas NetBIOS no servidor WINS, não podem ser utilizadas.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem SNMPv1, v2 não podem ser utilizadas. Utilizando o painel de controlo, o Web Image Monitor ou telnet, pode especificar as definições SNMPv1, v2 para só de leitura, não podendo ser editadas.

Protocolo	Porta	Método de definição	Quando desativado
SNMPv3	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem SNMPv3 não podem ser utilizadas. Pode também especificar definições para requerer uma transmissão encriptada SNMPv3 e restringir a utilização de outros métodos de transmissão utilizando o painel de controlo, o Web Image Monitor ou telnet.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que exijam RSH e as funções da rede TWAIN não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controlo utilizando "Restringir visualiz. informações utilizador".
LPR	TCP:515	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções LPR. É possível restringir a visualização de informações pessoais efetuando definições no painel de controlo utilizando "Restringir visualiz. informações utilizador".
IPP	TCP:631	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções IPP.
SSDP	UDP:1900	• Web Image Monitor • telnet	A localização de dispositivo utilizando UPnP a partir do Windows não pode ser utilizada.
Bonjour	UDP:5353	• Web Image Monitor • telnet	Não é possível utilizar funções Bonjour.

Protocolo	Porta	Método de definição	Quando desativado
@Remote	TCP:7443 TCP:7444	• Painel de controlo • telnet	Não é possível utilizar @Remote.
DIPRINT	TCP:9100	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções DIPRINT.
RFU	TCP:10021	• Painel de controlo • telnet	É possível atualizar firmware via FTP.
NetWare	(IPX/SPX)	• Painel de controlo • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível imprimir com NetWare. Não é possível utilizar SNMP através de IPX.
WSD (Equipamento)	TCP:53000 (variável)	• Web Image Monitor • telnet	Não é possível utilizar funções WSD (Equipamento).
WSD (Impressora)	TCP:53001 (variável)	• Web Image Monitor • telnet	Não é possível utilizar funções WSD (Impressora).
WS--Discovery	UDP/TCP: 3702	• telnet	A função de procura WSD (Device, Printer) não pode ser utilizada.
LLTD	-	• telnet	Não é possível utilizar a função de procura de equipamento utilizando LLTD.
LLMNR	UDP:5355	• Web Image Monitor • telnet	Não é possível responder a pedidos de resolução de nome utilizando LLMNR.

Nota

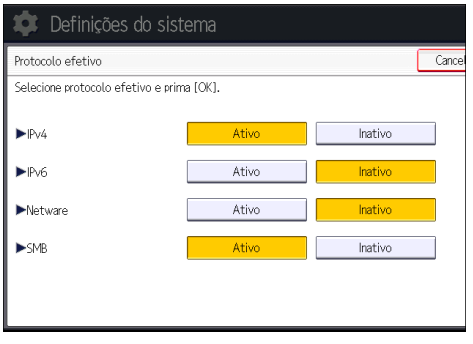
- "Restringir visualiz. informações utilizador" é uma das funções de Segurança Avançada. Para mais informações sobre como configurar esta definição, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".

Ativar e desativar protocolos utilizando o painel de controlo

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Defin. interface].**
4. **Prima [Protocolo efetivo].**



5. **Selecione o protocolo que pretende ativar ou desativar.**



6. **Prima [OK].**
7. **Encerre sessão.**

Ativar e desativar protocolos utilizando o Web Image Monitor

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**

3. **Clique em [Segurança da rede] sob "Segurança".**
4. **Selecione o protocolo que pretende ativar ou desativar ou selecione a porta que pretende abrir ou fechar.**
5. **Clique em [OK].**
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Especificar Níveis de Segurança da Rede

Esta definição permite alterar os níveis de segurança para limitar o acesso não autorizado. É possível configurar as definições de nível de segurança da rede utilizando o painel de controlo ou o Web Image Monitor. Note que os protocolos que podem ser especificados variam.

Importante

- **No caso de alguns utilitários, a comunicação ou o início de sessão podem falhar, dependendo do nível de segurança da rede.**

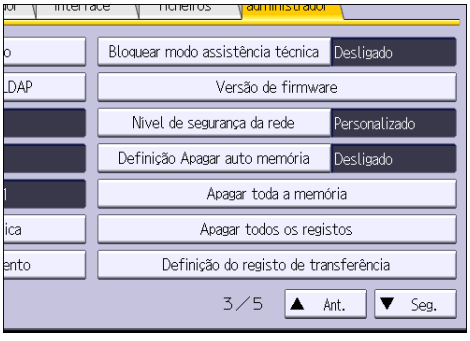
Níveis de segurança da rede

Nível de Segurança	Descrição
[Nível 0]	Selecione [Nível 0] para utilizar todas as funções. Utilize esta definição se não tiver informações que necessitem de ser protegidas contra ameaças externas.
[Nível 1]	Selecione [Nível 1] para segurança moderada e proteção de informações importantes. Utilize esta definição se o equipamento estiver ligado a uma rede local (LAN).
[FIPS140]	Fornece um grau de segurança intermédio, entre [Nível 1] e [Nível 2]. Apenas pode utilizar códigos recomendados pelo governo dos E.U.A. como algoritmo de codificação/autenticação. Outras definições que não o algoritmo correspondem ao [Nível 2].
[Nível 2]	Selecione [Nível 2] para segurança máxima e proteção de informações confidenciais. Utilize esta definição quando for necessário proteger informações contra ameaças externas.
[Personalizado]	Para outras configurações que não os níveis acima. Configure utilizando o Web Image Monitor.

Especificar os níveis de segurança de rede utilizando o painel de controlo

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] duas vezes.**

5. **Prima [Nível de segurança da rede].**



6. **Selecione o nível de segurança da rede pretendido.**

   Selecione [Nível 0], [Nível 1], [Nível 2] ou [FIPS140].

7. **Prima [OK].**
8. **Encerre sessão.**

Especificar o nível de segurança de rede utilizando o Web Image Monitor

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Segurança da rede] sob "Segurança".**
4. **Selecione o nível de segurança da rede em "Nível de segurança".**
5. **Clique em [OK].**
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.

7. **Encerre sessão.**

Estado das funções em cada nível de segurança da rede

TCP/IP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
TCP/IP	Ativo	Ativo	Ativo	Ativo
HTTP > Porta 80	Abrir	Abrir	Abrir	Abrir

Função	Nível 0	Nível 1	FIPS 140	Nível 2
IPP > Porta 80	Abrir	Abrir	Abrir	Abrir
IPP > Porta 631	Abrir	Abrir	Fechar	Fechar
SSL/TLS > Porta 443	Abrir	Abrir	Abrir	Abrir
SSL/TLS > Permitir comunicação SSL/TLS	Prioridade texto cifrado	Prioridade texto cifrado	Só texto cifrado	Só texto cifrado
Versão SSL/TLS > TLS1.2	Ativo	Ativo	Ativo	Ativo
Versão SSL/TLS > TLS1.1	Ativo	Ativo	Ativo	Ativo
Versão SSL/TLS > TLS1.0	Ativo	Ativo	Ativo	Ativo
Versão SSL/TLS > SSL3.0	Ativo	Ativo	Inativo	Inativo
Definição do grau de encriptação > AES	128 bits/256 bits	128 bits/256 bits	128 bits/256 bits	128 bits/256 bits
Definição do grau de encriptação > 3DES	168 bits	168 bits	168 bits	-
Definição do grau de encriptação > RC4	-	-	-	-
DIPRINT	Ativo	Ativo	Inativo	Inativo
LPR	Ativo	Ativo	Inativo	Inativo
FTP	Ativo	Ativo	Ativo	Ativo
sftp	Ativo	Ativo	Ativo	Ativo
ssh	Ativo	Ativo	Ativo	Ativo
RSH/RCP	Ativo	Ativo	Inativo	Inativo
TELNET	Ativo	Inativo	Inativo	Inativo
Bonjour	Ativo	Ativo	Inativo	Inativo
SSDP	Ativo	Ativo	Inativo	Inativo
SMB	Ativo	Ativo	Inativo	Inativo

Função	Nível 0	Nível 1	FIPS 140	Nível 2
NetBIOS sobre TCP/IPv4	Ativo	Ativo	Inativo	Inativo
WSD (Device)	Ativo	Ativo	Ativo	Ativo
WSD (Printer)	Ativo	Ativo	Ativo	Ativo
WSD (comunicação encriptada do equipamento)	Inativo	Inativo	Ativo	Ativo

As mesmas definições aplicam-se a IPv4 e IPv6.

A definição de TCP/IP não é controlada pelo nível de segurança. Especifique manualmente a ativação ou desativação desta definição.

NetWare

Função	Nível 0	Nível 1	FIPS 140	Nível 2
NetWare	Ativo	Ativo	Inativo	Inativo

Se o Netware não for utilizado na sua rede, as definições acima não se aplicam.

SNMP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
SNMP	Ativo	Ativo	Ativo	Ativo
Permitir definições por SNMPv1 e v2	Ligado	Desligado	Desligado	Desligado
Função SNMPv1,v2	Ativo	Ativo	Inativo	Inativo
Função SNMPv3	Ativo	Ativo	Ativo	Ativo
Permitir comunicação SNMPv3	Encriptação /Texto simples	Encriptação /Texto simples	Só encriptação	Só encriptação

Definição do grau de encriptação TCP/IP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
ssh > Algoritmo de encriptação	DES/3DES/ AES-128/ AES-192/ AES-256/ Blowfish/ Arcfour	3DES/ AES-128/ AES-192/ AES-256/ Arcfour	3DES/ AES-128/ AES-192/ AES-256	3DES/ AES-128/ AES-192/ AES-256
S/MIME > Algoritmo de encriptação	3DES-168 bit	3DES-168 bit	3DES-168 bit	AES de 256 bits
S/MIME > Algoritmo Digest	SHA1	SHA1	SHA1	SHA de 256 bits
SNMPv3 > Algoritmo de autenticação	MD5	SHA1	SHA1	SHA1
SNMPv3 > Algoritmo de encriptação	DES	DES	AES-128	AES-128
Autenticação Kerberos > Algoritmo de encriptação	AES256-CTS--HMAC--SHA1-96/ AES128-CTS--HMAC--SHA1-96/ DES3-CBC--SHA1/RC4--HMAC/DES--CBC-MD5	AES256-CTS--HMAC--SHA1-96/ AES128-CTS--HMAC--SHA1-96/ DES3-CBC--SHA1/RC4--HMAC	AES256-CTS--HMAC--SHA1-96/ AES128-CTS--HMAC--SHA1-96/ DES3-CBC--SHA1	AES256-CTS--HMAC--SHA1-96/ AES128-CTS--HMAC--SHA1-96
Chave de encriptação do driver > Grau de encriptação	Encriptação simples	DES	AES	AES

Proteger Vias de Comunicação com um Certificado de Dispositivo

Este equipamento pode proteger as suas próprias vias de comunicação e estabelecer comunicações encriptadas utilizando SSL/TLS, IPsec, S/MIME ou IEEE 802.1X. Pode também proteger PDFs utilizando uma assinatura digital de PDF ou PDF/A.

Para utilizar estas funções, é necessário criar e instalar previamente um certificado de dispositivo para o equipamento.

Podem ser utilizados os seguintes tipos de certificado de dispositivos:

- Certificados próprios criados pelo equipamento
- Certificados emitidos por uma autoridade de certificação

Importante

- **Cabe ao administrador gerir o prazo de validade dos certificados, bem como renovar os certificados antes de expirar o respetivo prazo de validade.**
- **O administrador deve verificar que o emissor do certificado é válido.**
- **Se SHA256 ou SHA512 estiver selecionado como "Algoritmo para assinatura" do certificado do dispositivo, é necessário o Windows XP SP3 ou superior para ligar o dispositivo utilizando o Internet Explorer 6.0.**

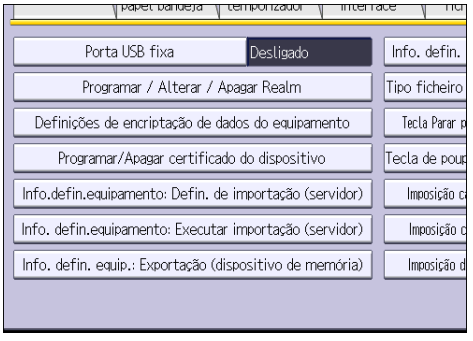
Criar e instalar um certificado de dispositivo a partir do painel de controlo (certificado próprio)

Crie e instale o certificado do dispositivo utilizando o painel de controlo.

Este capítulo explica a utilização de um certificado próprio como o certificado de dispositivo.

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**

5. **Prima [Programar/Apagar certificado do dispositivo].**


Porta USB fixa
Desligado
Info. defin.
Programar / Alterar / Apagar Realm
Tipo ficheiro
Definições de encriptação de dados do equipamento
Programar/Apagar certificado do dispositivo
Info.defin.equipamento: Defin. de importação (servidor)
Info. defin.equipamento: Executar importação (servidor)
Info. defin. equip.: Exportação (dispositivo de memória)

6. **Certifique-se de que [Programa] está selecionado.**
7. **Prima [Certificado 1].**

   Apenas [Certificado 1] pode ser criado a partir do painel de controlo.

8. **Configure as definições necessárias.**

   Para utilizar o certificado do equipamento para S/MIME, Assinatura digital de PDF ou Assinatura digital de PDF/A, introduza o endereço de e-mail do administrador do equipamento na definição de endereço de e-mail.

9. **Prima [OK].**

   "Instalado" aparece sob "Estado do certificado" para indicar que foi instalado um certificado de dispositivo para o equipamento.

10. **Encerre sessão.**

Nota

- Selecione [Apagar] para eliminar do equipamento o certificado do dispositivo.
- Para utilizar o certificado do dispositivo no equipamento para S/MIME ou Assinatura digital de PDF/A, defina "Certificação" no Web Image Monitor para [Certificado 1].

Criar e instalar um certificado de dispositivo a partir do Web Image Monitor (certificado próprio)

Crie e instale o certificado de dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens apresentados e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado próprio como o certificado de dispositivo.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**

4. **Selecione o botão de opção ao lado do número do certificado que pretende criar.**

   Para utilizar SSL/TLS, selecione [Certificado 1]. Para utilizar qualquer outro protocolo, selecione o número de certificado que pretende utilizar.

5. **Clique em [Criar].**

   Clique em [Apagar] para apagar o certificado de dispositivo do equipamento.

6. **Configure as definições necessárias.**

   Para utilizar o certificado do equipamento para S/MIME, Assinatura digital de PDF ou Assinatura digital de PDF/A, introduza o endereço de e-mail do administrador do equipamento na definição de endereço de e-mail.

7. **Clique em [OK].**

   A definição é alterada.

8. **Clique em [OK].**

9. **Se surgir uma mensagem de alerta de segurança, verifique os detalhes e selecione "Continuar para este website".**

   "Instalado" aparece sob "Estado do certificado" para indicar que foi instalado um certificado de dispositivo para o equipamento.

10. **Encerre sessão.**

Criar um certificado do dispositivo (emitido por uma autoridade de certificação)

Crie o certificado do dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens apresentados e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado emitido por uma autoridade de certificação como certificado de servidor.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o botão de opção ao lado do número do certificado que pretende criar.**

   Para utilizar SSL/TLS, selecione [Certificado 1]. Para utilizar qualquer outro protocolo, selecione o número de certificado que pretende utilizar.

5. **Clique em [Solicitar].**
6. **Configure as definições necessárias.**
7. **Clique em [OK].**

   A definição é alterada.

8. **Clique em [OK].**

   "A solicitar" aparece para "Estado do certificado".

9. **Encerre sessão.**

10. **Solicite um certificado de dispositivo à autoridade de certificação.**

    O processo do pedido depende da autoridade de certificação. Para mais informações, contacte a autoridade de certificação.

    Para a aplicação, clique no ícone Web Image Monitor Detalhes e utilize as informações apresentadas em "Detalhes do certificado".

Nota

- Se pedir 2 certificados em simultâneo, a origem da emissão pode não aparecer nos certificados. Quando instala um certificado, não se esqueça de verificar o destino e o processo de instalação do certificado.
- É possível utilizar o Web Image Monitor para criar o certificado do dispositivo, mas não para solicitar o certificado à autoridade de certificação.
- Clique em [Cancelar pedido] para cancelar o pedido de certificado de dispositivo.

Instalar um certificado de dispositivo (emitidos por uma autoridade de certificação)

Instale o certificado do dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens apresentados e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado emitido por uma autoridade de certificação como certificado de servidor.

Introduza o conteúdo da certificação do dispositivo emitida pela autoridade de certificação.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o botão de opção ao lado do número de certificado que pretende instalar.**

   Para utilizar SSL/TLS, selecione [Certificado 1]. Para utilizar qualquer outro protocolo, selecione o número de certificado que pretende utilizar.

5. **Clique em [Instalar].**
6. **Introduza o conteúdo da certificação do dispositivo.**

   Na caixa de certificação, introduza os conteúdos do certificado do dispositivo emitido pela autoridade de certificação.

   Se vai instalar um certificado intermédio, introduza também os conteúdos do certificado intermédio.

Para mais informações sobre os itens apresentados e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

7. **Clique em [OK].**
8. **Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   "Instalado" aparece sob "Estado do certificado" para indicar que foi instalado um certificado de dispositivo para o equipamento.
9. **Encerre sessão.**

Instalação de um certificado intermédio (emitido por uma autoridade de certificação)

Esta secção explica como utilizar o Web Image Monitor para instalar um certificado intermédio emitido por uma autoridade de certificação.

Se não possui o certificado intermédio emitido pela autoridade de certificação, aparecerá uma mensagem de aviso durante a comunicação. Se a autoridade de certificação emitiu um certificado intermédio, recomendamos que o instale.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o botão de opção ao lado do número de certificado que pretende instalar.**
5. **Clique em [Instalar certificado intermédio].**
6. **Introduza o conteúdo do certificado intermédio.**

   Na caixa de certificação, introduza os conteúdos do certificado intermédio emitido pela autoridade de certificação. Para obter detalhes acerca dos itens e definições de um certificado, consulte a Ajuda do Web Image Monitor.
7. **Clique em [OK].**
8. **Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

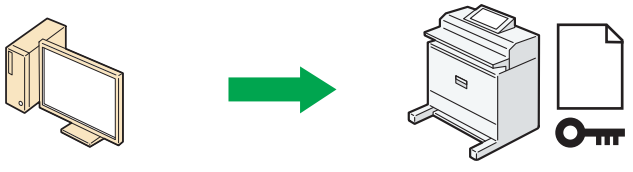
   O certificado intermédio será instalado no dispositivo. O ecrã "Detalhes do certificado" indicará se a instalação do certificado intermédio foi efetuada. Para mais informações sobre o ecrã "Detalhes do certificado", consulte a Ajuda do Web Image Monitor.
9. **Encerre sessão.**

Configurar as Definições SSL/TLS

Configurar o equipamento para utilizar SSL/TLS ativa as comunicações encriptadas. Este passo ajuda a prevenir a interceção, descodificação ou manipulação dos dados durante a transmissão.

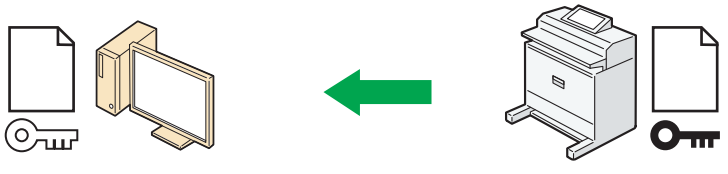
Sequência das comunicações encriptadas SSL/TLS

1. Para aceder ao equipamento a partir do computador de um utilizador, solicite um certificado de dispositivo SSL/TLS e uma chave pública.



CRX003

2. A certificação de dispositivo e o código público são enviados pelo equipamento para o computador do utilizador.



CRX004

3. O código partilhado criado com o computador é encriptado utilizando o código público, enviado ao equipamento e, em seguida, desencriptado utilizando o código privado no equipamento.



CRX005

4. O código partilhado é utilizado para a encriptação e desencriptação de dados, conseguindo deste modo uma transmissão segura.



CRX006

Sequência de configuração quando é utilizado um certificado auto-assinado

1. Criar e instalar o certificado do dispositivo:

   Crie e instale um certificado de dispositivo a partir do painel de controlo ou do Web Image Monitor.

2. Ativar SSL/TLS:

   Ative a definição SSL/TLS com Web Image Monitor.

Sequência de configuração quando é utilizado um certificado emitido por uma autoridade

1. Criar um certificado de dispositivo e enviar um pedido à autoridade:

   Depois de criar um certificado de dispositivo no Web Image Monitor, envie um pedido à autoridade de certificação.

   O procedimento do pedido após a criação do certificado depende da autoridade de certificação. Siga o procedimento especificado pela autoridade de certificação.

2. Instalar o certificado de dispositivo:

   Instale o certificado do dispositivo utilizando o Web Image Monitor.

3. Ativar SSL/TLS:

   Ative a definição SSL/TLS com Web Image Monitor.

Nota

- Para verificar se a configuração SSL/TLS está ativada, introduza "https://(o endereço IP ou o nome de host do equipamento)/" na barra de endereços do web browser para aceder a este equipamento. Se aparecer a mensagem "A página não pode ser visualizada", verifique a configuração, porque a configuração SSL/TLS atual não é válida.
- Se ativar SSL/TLS para IPP (funções de impressora), os dados enviados são encriptados, o que impede que sejam interceptados, analisados ou manipulados.

Ativar SSL/TLS

Depois de instalar um certificado de dispositivo no equipamento, ative a definição de SSL/TLS.

Este procedimento é utilizado para um certificado próprio ou para um certificado emitido por uma autoridade de certificação.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [SSL/TLS] em "Segurança".**
4. **Para IPv4 e IPv6, selecione "Ativo" caso pretenda ativar SSL/TLS.**
5. **Selecione o modo de comunicação de encriptação para "Permitir comunicação SSL/TLS".**

6. **Se pretender desativar um protocolo, clique em [Inativo] junto a "TLS1.2", "TLS1.1", "TLS1.0" ou "SSL3.0".**

   Pelo menos um destes protocolos tem de ser ativado.

7. **Sob "Definição do grau de encriptação", especifique o grau de encriptação a ser aplicado para "AES", "3DES" e/ou "RC4". Tem de selecionar, pelo menos, uma caixa de seleção.**

   Note que a disponibilidade de graus de encriptação varia consoante as definições especificadas para "TLS1.2", "TLS1.1", "TLS1.0" ou "SSL3.0".

8. **Clique em [OK].**

9. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.

10. **Encerre sessão.**

Nota

- Se definir "Permitir comunicação SSL/TLS" como [Só texto cifrado], a comunicação não será possível se selecionar um protocolo que não suporte um Web browser ou se especificar apenas uma definição do grau de encriptação. Se tal for o caso, ative a comunicação através da definição [Permitir comunicação SSL/ TLS] para [Texto cifrado/simples] usando o painel de controlo do equipamento e especificando o protocolo e grau de encriptação corretos.
- É possível alterar as definições de versão SSL/TLS e grau de encriptação mesmo em [Segurança da rede].
- Dependendo dos estados que especificar para "TLS1.2", "TLS1.1", "TLS1.0" e "SSL3.0", o equipamento pode não conseguir ligar a um servidor LDAP externo.
- Os seguintes tipos de comunicação e dados são sempre encriptados por SSL3.0: comunicação via @Remote e registos transferidos para a Remote Communication Gate S.

Definição de utilizador para SSL/TLS

Recomendamos que, após a instalação de um certificado próprio ou certificado de dispositivo de uma autoridade de certificação privada na unidade principal e após a ativação da função SSL/TLS (encriptação de comunicações), sejam dadas instruções aos utilizadores para procederem à instalação do certificado nos respetivos computadores. É necessária a instalação do certificado especialmente para utilizadores que pretendam imprimir via IPP-SSL a partir do Windows Vista/7/8/8.1, Windows Server 2008/2008 R2/2012/2012 R2. O administrador da rede deve instruir cada utilizador para que instale o certificado.

Selecione [Autoridades de certificação de raiz fidedignas] para obter a localização da loja de certificados quando aceder ao equipamento por IPP.

Nota

- Tome medidas adequadas no caso de receber questões do utilizador relativas a problemas como um certificado expirado.
- Se um certificado emitido por uma autoridade de certificação estiver instalado no equipamento, verifique o local de armazenamento do certificado com a autoridade de certificação.
- Para alterar o nome do host ou endereço IP em [Nome comum] do certificado do dispositivo quando utilizar a porta IPP standard do sistema operativo no Windows Vista/7/8/8.1 ou Windows Server 2008/2008 R2/2012/2012 R2, elimine todas as impressoras de PC previamente configuradas e reinstale após alterar o [Nome comum]. Para alterar as definições de autenticação do utilizador (nome de utilizador e palavra-passe), elimine todas as impressoras de PC previamente configuradas e reinstale após alterar as definições de autenticação do utilizador.

Definir modo de encriptação SSL/TLS

Ao especificar o modo de comunicação encriptada SSL/TLS, pode alterar os níveis de segurança.

Modo de comunicação encriptada

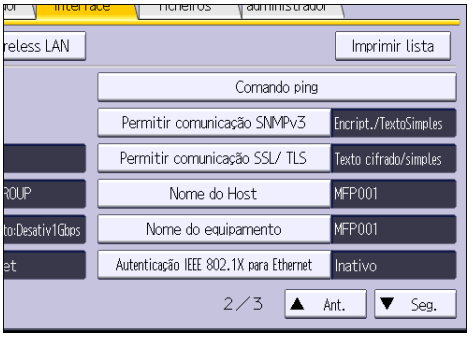
Utilizando o modo de comunicação encriptada, pode especificar comunicações encriptadas.

Modo de comunicação encriptada	Descrição
Só texto cifrado	Permite apenas a comunicação encriptada. Se a encriptação não for possível, o equipamento não comunica.
Prioridade texto cifrado	Efetua a comunicação encriptada se a encriptação for possível. Se a encriptação não for possível, o equipamento comunica de qualquer forma.
Texto cifrado/simples	Comunica com ou sem encriptação, de acordo com as definições.

Depois de instalar um certificado do dispositivo, especifique o modo de comunicação encriptada SSL/TLS. Ao configurar esta definição, pode alterar o nível de segurança.

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Defin. interface].**
4. **Prima [▼Seg.].**

5. **Prima [Permitir comunicação SSL/ TLS].**



6. **Selecione o modo de comunicação encriptada do equipamento que pretende utilizar.**

   Selecione [Só texto cifrado], [Prioridade texto cifrado] ou [Texto cifrado/simples] como o modo de comunicação encriptada.

7. **Prima [OK].**

8. **Encerre sessão.**

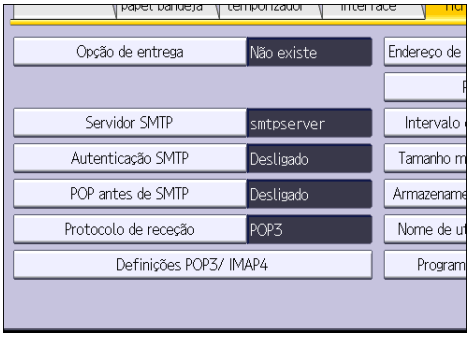
Nota

- O modo de comunicação encriptada SSL/TLS também pode ser especificado utilizando o Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Ativar SSL para Ligações SMTP

Utilize o procedimento seguinte para ativar a encriptação SSL para as ligações SMTP.

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Transfer. ficheiros].**
4. **Prima [Servidor SMTP].**



5. **Em "Utilizar ligação segura (SSL)", prima [Ligado].**

   Se não usar SSL para ligações SMTP, prima [Desligado].

   Quando "Utilizar ligação segura (SSL)" estiver definido como [Ligado], o número da porta muda para 465.

6. **Prima [OK].**
7. **Encerre sessão.**

Configurar S/MIME

Registando uma certificação de utilizador no livro de endereços, pode enviar um e-mail encriptado com uma chave pública que evita que o respetivo conteúdo seja alterado durante a transmissão. Também pode evitar uma imitação do emissor (spoofing) instalando um certificado de dispositivo no equipamento e juntando uma assinatura eletrónica criada com uma chave privada. Pode aplicar estas funções separadamente ou, para uma maior segurança, em conjunto.

Para enviar e-mails encriptados, tanto o emissor (este equipamento) como o recetor devem suportar S/MIME.

Importante

- **Para utilizar S/MIME, tem primeiro de especificar [Endereço de e-mail do administrador] em [Definições do sistema].**

Aplicações mailer compatíveis

A função S/MIME pode ser utilizada com as seguintes aplicações:

- Microsoft Outlook 2003 e posterior
- Thunderbird 3.1.7 e posterior
- Windows Live Mail

Nota

- Se uma assinatura eletrónica está especificada para um e-mail, o endereço do administrador aparece no campo "De" e o endereço do utilizador especificado como "remetente" aparece no campo "Responder a".
- Quando envia e-mails para utilizadores cujos clientes de correio suportam S/MIME e utilizadores cujos clientes não suportam S/MIME, os e-mails para clientes S/MIME são encriptados e os e-mails para clientes não S/MIME são enviados como texto simples.
- Ao utilizar S/MIME, o tamanho do e-mail é maior do que o normal.
- Para mais informações acerca da utilização de S/MIME com a função de scanner, consulte Digitalização.

Encriptação de e-mail

Para enviar e-mails encriptados utilizando S/MIME, deve ser preparado em primeiro lugar um certificado de utilizador, através do Web Image Monitor e registado no livro de endereços pelo administrador de utilizadores. Registar o certificado no livro de endereços especifica a chave pública de cada utilizador. Depois de instalar o certificado, especifique o algoritmo de encriptação utilizando o Web Image Monitor. O administrador da rede pode especificar o algoritmo.

Encriptação de e-mail

1. Prepare um certificado de utilizador.

2. Instale a certificação de utilizador no livro de endereços utilizando o Web Image Monitor. (A chave pública da certificação é especificada no livro de endereços.)
3. Especifique o algoritmo de encriptação utilizando o Web Image Monitor.
4. Utilizando a chave partilhada, encripte a mensagem de e-mail.
5. A chave partilhada é encriptada utilizando a chave pública do utilizador.
6. O e-mail encriptado é enviado.
7. O recetor desencripta a chave partilhada utilizando uma chave secreta que corresponde à chave pública.
8. O e-mail é desencriptado utilizando a chave partilhada.

Nota

- Existem 3 tipos de certificados de utilizador que podem ser instalados neste equipamento: "DER Encoded Binary X.509", "Base 64 Encoded X.509" e "PKCS #7".
- Ao instalar um certificado de utilizador no livro de endereços utilizando o Web Image Monitor, poderá aparecer uma mensagem de erro se o ficheiro de certificado tiver mais do que um certificado. Nesse caso, instale os certificados um de cada vez.

Especificar o certificado de utilizador

Prepare previamente cada certificado de utilizador.

1. **Inicie sessão como administrador de utilizadores a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Livro de endereços].**
3. **Selecionar o utilizador para quem o certificado será instalado.**
4. **Clique em [Introdução detalhada] e, em seguida, clique em [Alterar].**

   Aparece o ecrã Alterar utilizador.
5. **Introduza o endereço do utilizador no campo "Endereço de e-mail" em "E-mail".**
6. **Clique em [Alterar] em "Certificado do utilizador".**
7. **Clique em [Procurar], selecione o ficheiro de certificado do utilizador e, em seguida, clique em [Abrir].**
8. **Clique em [OK].**

   O certificado de utilizador é instalado.
9. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
10. **Encerre sessão.**

Nota

- Quando o prazo de validade do certificado do utilizador selecionado expirar, deixa de ser possível enviar mensagens encriptadas. Selecione um certificado cujo prazo de validade esteja válido.

Especificar o algoritmo de encriptação

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [S/MIME] sob "Segurança".**
4. **Selecione o algoritmo de encriptação no menu junto a "Algoritmo de encriptação" em "Encriptação".**
5. **Clique em [OK].**

   É definido o algoritmo para S/MIME.
6. **Encerre sessão.**

Nota

- Configure as definições, tendo em consideração o algoritmo de encriptação e o algoritmo digest suportados pelo software de e-mail do utilizador.

Juntar uma assinatura eletrónica

Para juntar uma assinatura eletrónica a um e-mail a enviar, deve ser previamente instalado um certificado de dispositivo.

Como certificado do dispositivo, pode utilizar um certificado próprio criado pelo equipamento ou um certificado emitido por uma autoridade de certificação. Para mais informações sobre como criar e instalar o certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo".

Importante

- **Para instalar um certificado de dispositivo S/MIME, tem de registar primeiro "Endereço de e-mail do administrador" em [Definições do sistema] como endereço de email para o certificado de dispositivo. Tenha em atenção que, se não utilizar o S/MIME, será necessário especificar um endereço de e-mail para o certificado do dispositivo S/MIME.**

Assinatura eletrónica

1. Instale um certificado do dispositivo no equipamento. A chave secreta do certificado é configurada no equipamento.
2. Junte a assinatura eletrónica a um e-mail utilizando a chave secreta fornecida pelo certificado de dispositivo.

3. Envie o e-mail com a assinatura eletrónica anexada ao utilizador.
4. O recetor pede ao equipamento a chave pública e o certificado de dispositivo.
5. Utilizando a chave pública, pode determinar a autenticidade da assinatura eletrónica anexa para verificar se a mensagem foi alterada.

Fluxo da configuração (certificado próprio)

1. Crie e instale o certificado de dispositivo utilizando o Web Image Monitor.
2. Configure as definições do certificado a utilizar pelo S/MIME com o Web Image Monitor.
3. Configure as definições da assinatura eletrónica utilizando o Web Image Monitor.

Fluxo da configuração (certificado emitido por uma autoridade de certificação)

1. Crie o certificado do dispositivo utilizando o Web Image Monitor.

   O procedimento de solicitação para um certificado criado depende da autoridade de certificação. Siga o procedimento especificado pela autoridade de certificação.
2. Instale o certificado do dispositivo utilizando o Web Image Monitor.
3. Configure as definições do certificado a utilizar pelo S/MIME com o Web Image Monitor.
4. Configure as definições da assinatura eletrónica utilizando o Web Image Monitor.

Selecionar o certificado do dispositivo

Selecione o certificado do dispositivo utilizar para S/MIME com o Web Image Monitor.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o certificado a utilizar para a assinatura eletrónica na caixa em "S/MIME", "Certificação".**
5. **Clique em [OK].**

   É definida o certificado utilizar para a assinatura eletrónica do S/MIME.
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Nota

- Se o certificado do dispositivo selecionado expirar, não será possível anexar assinaturas a e--mails. Selecione um certificado cujo prazo de validade esteja válido.

Especificar a assinatura eletrónica

Após instalar um certificado de dispositivo para este equipamento, configure as condições para assinaturas S/MIME. O procedimento de configuração é o mesmo independentemente de utilizar um certificado próprio ou um certificado emitido por uma autoridade de certificação.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [S/MIME] sob "Segurança".**
4. **Selecione o algoritmo digest a ser utilizado na assinatura eletrónica junto a "Algoritmo Digest" em "Assinatura".**
5. **Selecione o método para anexar a assinatura eletrónica quando enviar e-mail a partir do scanner junto a "Quando enviar e-mail via scanner" em "Assinatura".**
6. **Selecione o método para juntar a assinatura eletrónica quando reencaminhar documentos guardados junto a "Quando transferir ficheiros guardados no servidor de documentos (Utilitário)" em "Assinatura".**
7. **Clique em [OK].**

   São ativadas as definições da assinatura eletrónica S/MIME.
8. **Encerre sessão.**

Nota

- Configure as definições com base no algoritmo de encriptação e o algoritmo digest suportados pelo software de e-mail do utilizador.

Verificar o período de validade do certificado

O período de validade de um certificado utilizado com S/MIME é verificado quando envia um e-mail.

Pode alterar o momento no qual o período de validade é verificado.

Modo de operação	Descrição
Prioridade de segurança	O período de validade é verificado com a frequência seguinte: **Certificação de Utilizador** (a) Quando o endereço é selecionado (b) Quando a tecla [Iniciar] é premida **Certificação do dispositivo** (c) Quando o primeiro endereço é selecionado (d) Quando a tecla [Iniciar] é premida

Modo de operação	Descrição
Prioridade de desempenho	Os passos (b) e (c) são omitidos. Se o endereço for selecionado ou a tecla [Iniciar] for premida, a verificação do período de validade pode demorar mais tempo. Para reduzir o tempo necessário para o processo, selecione "Prioridade de desempenho".

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [S/MIME] sob "Segurança".**
4. **Em "Modo de Operação", selecione [Prioridade de segurança] ou [Prioridade de desempenho].**
5. **Clique em [OK].**
6. **Encerre sessão.**

Nota

- Se um certificado era válido durante a transmissão, mas expirou antes de obter o e-mail do servidor de e-mail para o computador cliente, o e-mail poderá não ser recuperado.
- Se ocorrer um erro após o período de validade do certificado ao enviar automaticamente um e-mail S/MIME utilizando a transmissão por memória ou num determinado momento, o erro será comunicado por e-mail em texto não encriptado para o endereço de e-mail do remetente ou do administrador. Os detalhes do erro podem ser visualizados no registo de trabalhos. Quando utilizar S/MIME, certifique-se de que ativa a função de recolha do registo de trabalhos. Para mais informações sobre como consultar os registos, consulte Pág. 177 "Gerir Ficheiros de Registo".

Configurar PDFs com Assinaturas Eletrónicas

Este equipamento pode criar PDFs com assinaturas eletrónicas. PDFs com assinaturas eletrónicas certificam o criador do documento PDF e a data e hora da criação. A adulteração é também impedida porque é possível detetar os documentos que tenham sido adulterados.

Para criar PDFs com assinaturas eletrónicas, primeiro selecione o certificado a utilizar para a assinatura a partir dos certificados de dispositivo que foram criados e instalados.

Como certificado do dispositivo, pode utilizar um certificado próprio criado pelo equipamento ou um certificado emitido por uma autoridade de certificação. Para mais informações sobre como criar e instalar um certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo".

Importante

- **Para criar PDF assinados digitalmente tem primeiro de especificar o [Endereço e-mail do admin] em [Transfer. ficheiros] nas [Definições do sistema].**
- **Para utilizar o certificado do equipamento para PDF assinados digitalmente tem primeiro de especificar o endereço de e-mail do administrador de forma a que seja o mesmo introduzido em "Endereço e-mail do admin" nas [Definições do sistema].**

Selecione o certificado a utilizar para assinaturas.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o certificado a ser utilizado para a assinatura eletrónica a partir da caixa em "Assinatura digital de PDF" ou "Assinatura digital de PDF/A", em "Certificação".**

   Assinatura digital de PDF: pode ser anexada a PDFs noutros formatos que não PDF/A.

   Assinatura digital de PDF/A: pode ser anexada a PDFs no formato PDF/A.
5. **Clique em [OK].**
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Nota

- Se o certificado do dispositivo selecionado expirar, não é possível anexar assinaturas a PDFs. Selecione um certificado cujo prazo de validade esteja válido.
- O algoritmo de assinatura da assinatura digital do certificado do dispositivo que pode ser anexada a ficheiros PDF/A é "sha1WithRSA-1024".

Configurar Definições IPsec

Para a segurança das comunicações, este equipamento suporta IPsec. IPsec transmite pacotes de dados seguros ao nível do protocolo IP utilizando o método de código de encriptação partilhado, no qual o remetente e o destinatário possuem o mesmo código. Este equipamento utiliza uma chave de encriptação negociada automaticamente para configurar a chave pré-partilhada para ambas as partes. Utilizando a definição de negociação automática, pode renovar as definições de chave negociada automaticamente partilhada dentro de um período de tempo especificado e assim obter uma maior segurança na transmissão.

Importante

- **Quando for especificado "Inativo" para "Excluir comunicação HTTPS", o acesso ao Web Image Monitor pode ser perdido se as definições do código estiverem configuradas de forma incorreta. Para evitar que tal aconteça, pode especificar que o IPsec exclua a transmissão HTTPS selecionando "Ativo". Quando pretender incluir a transmissão HTTPS, recomendamos que selecione "Inativo" para "Excluir comunicação HTTPS" após confirmar que o IPsec está devidamente configurado. Quando "Ativo" estiver selecionado para "Excluir comunicação HTTPS", apesar da transmissão HTTPS não ser abrangida pelo IPsec, o Web Image Monitor poderá ficar inacessível quando o TCP for abrangido pelo IPsec a partir do lado do computador.**
- **Se não conseguir aceder ao Web Image Monitor devido a problemas de configuração do IPsec, desative o IPsec nas Definições do sistema no painel de controlo e, em seguida, aceda ao Web Image Monitor.**
- **Para mais informações sobre a ativação e desativação do IPsec utilizando o painel de controlo, consulte Connecting the Machine/ System Settings.**
- **IPsec não é aplicado a dados obtidos através de DHCP, DNS ou WINS.**

Sistemas operativos suportados

Sistemas operativos	Nota
• Windows XP SP2/SP3 • Windows Server 2003/2003 R2	É possível utilizar IPsec sobre IPv4.
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 ou posterior • Red Hat Enterprise Linux WS 4.0 • Solaris 10	É possível utilizar IPsec sobre IPv4 e IPv6.

Alguns itens de definição não são suportados, dependendo do sistema operativo. Certifique-se de que as definições IPsec que especificar são consistentes com as definições IPsec do sistema operativo.

Encriptação e autenticação por IPsec

O IPsec consiste em 2 funções principais: a função de encriptação, que assegura a confidencialidade dos dados, e a função de autenticação, que verifica o remetente dos dados e a integridade dos mesmos. A função IPsec deste equipamento suporta 2 protocolos de segurança: o protocolo ESP, que ativa as duas funções do IPsec em simultâneo e o protocolo AH, que ativa apenas a função de autenticação.

Protocolo ESP

O protocolo ESP oferece uma transmissão segura através de autenticação e encriptação. Este protocolo não fornece autenticação do cabeçalho.

- Para uma encriptação bem sucedida, tanto o remetente como o destinatário têm de especificar o mesmo algoritmo de encriptação e chave de encriptação. Se utilizar o método de chave de encriptação negociada automaticamente, o algoritmo de encriptação e a chave de encriptação são especificados automaticamente.
- Para uma autenticação bem sucedida, tanto o remetente como o destinatário têm de especificar o mesmo algoritmo de autenticação e código de autenticação. Se utilizar o método de chave de encriptação negociado automaticamente, o algoritmo de autenticação e o código de autenticação são especificados automaticamente.

Protocolo AH

O protocolo AH oferece uma transmissão segura através da autenticação de apenas pacotes, incluindo cabeçalhos.

- Para uma autenticação bem sucedida, tanto o remetente como o destinatário têm de especificar o mesmo algoritmo de autenticação e código de autenticação. Se utilizar o método de chave de encriptação negociado automaticamente, o algoritmo de autenticação e o código de autenticação são especificados automaticamente.

Protocolo AH + Protocolo ESP

Quando combinados, os protocolos ESP e AH oferecem uma transmissão segura através de encriptação e autenticação. Estes protocolos oferecem autenticação de cabeçalho.

- Para uma encriptação bem sucedida, tanto o remetente como o destinatário têm de especificar o mesmo algoritmo de encriptação e chave de encriptação. Se utilizar o método de chave de encriptação negociada automaticamente, o algoritmo de encriptação e a chave de encriptação são especificados automaticamente.
- Para uma autenticação bem sucedida, tanto o remetente como o destinatário têm de especificar o mesmo algoritmo de autenticação e código de autenticação. Se utilizar o método de chave de encriptação negociado automaticamente, o algoritmo de autenticação e o código de autenticação são especificados automaticamente.

Nota

- Alguns sistemas operativos utilizam o termo "Conformidade" em vez de "Autenticação".

Definições da chave de encriptação negociada automaticamente

Para a configuração da chave, este equipamento suporta a negociação automática de chave de encriptação para especificar acordos tais como o algoritmo IPsec e chaves para o emissor e para o recetor. Este tipo de acordo forma aquilo que é conhecido como SA (Security Association). A comunicação IPsec é apenas possível se as definições SA do destinatário e do remetente forem idênticas.

Se utilizar o método de chave de encriptação negociada automaticamente para especificar a chave de encriptação, as definições SA são configuradas automaticamente nos equipamentos dos dois lados. Contudo, antes de definir a SA do IPsec, as definições SA ISAKMP (Fase 1) são configuradas automaticamente. Depois disto, as definições SA do IPsec (Fase 2), que permitem a transmissão IPsec, são configuradas automaticamente.

Além disso, para maior segurança, o SA pode ser atualizado de forma automática periodicamente aplicando um período de validade (limite de tempo) para as suas definições. Este equipamento suporta apenas IKEv1 para o código de encriptação negociado automaticamente.

Tenha em conta que é possível configurar vários multiple SAs.

Definições 1-4 e predefinição

Utilizando o método de chave de encriptação negociada automaticamente, pode configurar quatro conjuntos diferentes de detalhes SA (como chaves partilhadas e algoritmos IPsec diferentes). Nas predefinições destes conjuntos pode incluir definições não abrangidas pelos campos dos conjuntos 1-4.

Quando IPsec estiver ativado, o conjunto 1 tem a maior prioridade e o conjunto 4 a menor prioridade. Pode utilizar este sistema de prioridades para visar endereços IP de forma mais segura. Por exemplo, defina o intervalo IP maior para a prioridade mais baixa (4) e depois defina endereços IP específicos para um nível de prioridade mais elevado (3 e superior). Deste modo, quando a transmissão IPsec estiver ativada para um endereço IP específico, serão aplicadas as definições do nível mais elevado.

Definições IPsec

As definições IPsec para este equipamento podem ser efetuadas no Web Image Monitor. A seguinte tabela explica os itens individuais de definição.

Itens de definição IPsec

Definição	Descrição	Valor de definição
IPsec	Especifique se ativa ou não IPsec.	• Ativo • Inativo

Definição	Descrição	Valor de definição
Excluir comunicação HTTPS	Especifique se ativa IPsec para a transmissão HTTPS.	• Ativo • Inativo Especifique "Ativo" se não pretender utilizar IPsec para transmissão HTTPS.

A definição IPsec pode também ser configurada a partir do painel de controlo.

Nível de segurança do código de encriptação negociado automaticamente

Quando seleciona o nível de segurança, algumas definições de segurança são configuradas automaticamente. A tabela seguinte explica as funções dos níveis de segurança.

Nível de segurança	Funções do nível de segurança
Autenticação apenas	Selecione este nível se pretender autenticar o interlocutor da transmissão e evitar a manipulação não autorizada dos dados, mas não pretender efetuar a encriptação do pacote de dados. Como os dados são enviados em texto simples, os pacotes de dados são vulneráveis a ataques de escuta. Não selecione esta opção se estiver a trocar informações delicadas.
Autenticação e baixa encriptação	Selecione este nível se pretender encriptar os pacotes de dados assim como autenticar o interlocutor da transmissão e evitar a manipulação não autorizada do pacote. A encriptação de pacotes ajuda a evitar os ataques de escuta. Este nível proporciona menos segurança do que "Autenticação e elevada encriptação".
Autenticação e elevada encriptação	Selecione este nível se pretender encriptar os pacotes de dados assim como autenticar o interlocutor da transmissão e evitar a manipulação não autorizada do pacote. A encriptação de pacotes ajuda a evitar os ataques de escuta. Este nível proporciona uma segurança mais elevada do que "Autenticação e baixa encriptação".

A tabela seguinte lista as definições que são configuradas automaticamente de acordo com o nível de segurança.

Definição	Autenticação apenas	Autenticação e baixa encriptação	Autenticação e elevada encriptação
Política de segurança	Aplicar	Aplicar	Aplicar
Modo de encapsulamento	Transport	Transport	Transport
Nível de requisitos IPsec	Utilizar quando possível	Utilizar quando possível	Exigir sempre
Método de autenticação	PSK	PSK	PSK
Fase 1 Algoritmo Hash	MD5	SHA1	SHA256
Fase 1 Algoritmo de encriptação	DES	3DES	AES-128-CBC
Fase 1 Grupo Diffie-Hellman	2	2	2
Fase 2 Protocolo de segurança	AH	ESP	ESP
Fase 2 Algoritmo de autenticação	HMAC-SHA1-96/ HMAC- -SHA256-128/ HMAC- -SHA384-192/ HMAC- -SHA512-256	HMAC-SHA1-96/ HMAC- -SHA256-128/ HMAC- -SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
Fase 2 Permissões do algoritmo de encriptação	Texto simples (Encriptação NULL)	3DES/AES-128/ AES-192/AES-256	AES-128/AES-192/ AES-256
Fase 2 PFS	Inativo	Inativo	2

Itens das definições do código de encriptação negociado automaticamente

Quando especifica um nível de segurança, as definições de segurança correspondentes são configuradas automaticamente, mas outras definições, tal como o tipo de endereço, endereço local e endereço remoto, continuam a ter de ser definidas manualmente.

Depois de especificar um nível de segurança, continua a poder efetuar alterações às definições configuradas automaticamente. Quando altera uma definição configurada automaticamente, o nível de segurança muda automaticamente para "Definição do utilizador".

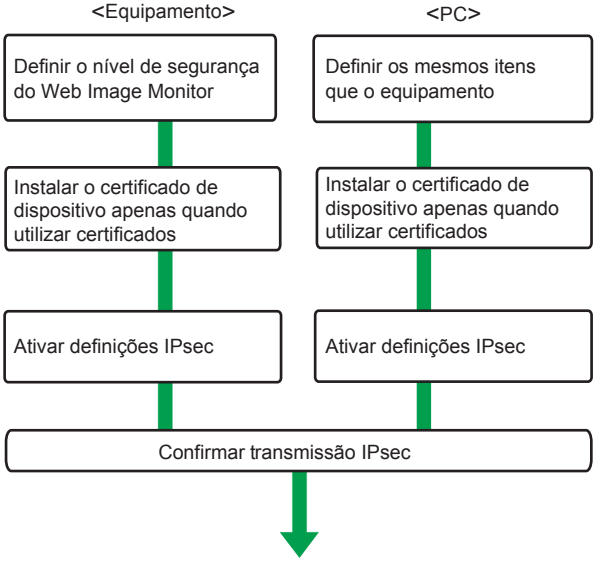
Definição	Descrição	Valor de definição
Tipo de endereço	Especifique o tipo de endereço para o qual é utilizada a transmissão IPsec.	• Inativo • IPv4 • IPv6 • IPv4/IPv6 (apenas Predefinições)
Endereço local	Especifique o endereço do equipamento. Se estiver a utilizar vários endereços IPv6, pode também especificar um intervalo de endereços.	O endereço IPv4 ou IPv6 do equipamento. Se não definir um intervalo de endereços, introduza 32 depois de um endereço IPv4 ou introduza 128 depois de um endereço IPv6.
Endereço remoto	Especifique o endereço do interlocutor da transmissão IPsec. Pode também especificar um intervalo de endereços.	O endereço IPv4 ou IPv6 do interlocutor da transmissão IPsec. Se não definir um intervalo de endereços, introduza 32 depois de um endereço IPv4 ou introduza 128 depois de um endereço IPv6.
Política de segurança	Especifique como o IPsec é gerido.	• Aplicar • Contornar • Descartar
Modo de encapsulamento	Especifique o modo de encapsulamento. (definição automática)	• Transport • Tunnel Se especificar "Tunnel", terá depois de especificar "Ponto de fim Tunnel", que consiste dos endereços IP de início e fim. Para o ponto de início, defina o endereço definido em "Endereço local".

Definição	Descrição	Valor de definição
Nível de requisitos IPsec	Especifique se pretende transmitir apenas através de IPsec ou se pretende a transmissão de texto simples quando não for possível estabelecer IPsec. (definição automática)	• Utilizar quando possível • Exigir sempre
Método de autenticação	Especifique o método de autenticação para os interlocutores da transmissão. (definição automática)	• PSK • Certificado Se especificar "PSK", terá depois de definir o texto PSK (utilizando carateres ASCII). Se estiver a utilizar "PSK", especifique uma palavra-passe PSK utilizando até 32 carateres ASCII. Se especificar "Certificado", o certificado para IPsec tem de ser instalado e especificado antes de poder ser utilizado.
Texto PSK	Especificar a chave pré-partilhada para autenticação PSK.	Introduza o código partilhado necessário para a autenticação PSK.
Fase 1 Algoritmo Hash	Especifique o algoritmo hash a ser utilizado na fase 1. (definição automática)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
Fase 1 Algoritmo de encriptação	Especifique o algoritmo de encriptação a ser utilizado na fase 1. (definição automática)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC

Definição	Descrição	Valor de definição
Fase 1 Grupo Diffie-Hellman	Selecione o número do grupo Diffie-Hellman utilizado para a criação de código de encriptação IKE. (definição automática)	• 1 • 2 • 14
Fase 1 Período de validade	Especifique o período de tempo pelo qual as definições SA na fase 1 serão válidas.	Defina, em segundos, de 300 seg. (5 min.) a 172 800 seg. (48 horas).
Fase 2 Protocolo de segurança	Especifique o protocolo de segurança a ser utilizado na fase 2. Para aplicar a encriptação e a autenticação a dados enviados, especifique o "ESP" ou o "ESP+AH". Para aplicar apenas dados de autenticação, especifique o "AH". (definição automática)	• ESP • AH • ESP+AH
Fase 2 Algoritmo de autenticação	Especifique o algoritmo de autenticação a ser utilizado na fase 2. (definição automática)	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Fase 2 Permissões do algoritmo de encriptação	Especifique o algoritmo de encriptação a ser utilizado na fase 2. (definição automática)	• Texto simples (Encriptação NULL) • DES • 3DES • AES-128 • AES-192 • AES-256

Definição	Descrição	Valor de definição
Fase 2 PFS	Especifique se pretende ativar PFS. De seguida, se PFS estiver ativado, selecione o grupo Diffie-Hellman. (definição automática)	• Inativo • 1 • 2 • 14
Fase 2 Período de validade	Especifique o período de tempo pelo qual as definições SA na fase 2 serão válidas.	Especifique um período (em segundos) de 300 (5 min.) a 172.800 (48 horas).

Sequência de configuração das Definições da chave de encriptação negociada automaticamente


<Equipamento>
<PC>
Definir o nível de segurança do Web Image Monitor
Definir os mesmos itens que o equipamento
Instalar o certificado de dispositivo apenas quando utilizar certificados
Instalar o certificado de dispositivo apenas quando utilizar certificados
Ativar definições IPsec
Ativar definições IPsec
Confirmar transmissão IPsec
PT CJD015

Importante

- Para utilizar um certificado para autenticar o interlocutor da transmissão nas definições de chave de encriptação negociada automaticamente, é necessário encontrar-se instalado um certificado do dispositivo.
- Depois de configurar o IPsec, pode utilizar o comando "Ping" para verificar se a ligação está estabelecida corretamente. No entanto, não pode utilizar o comando "Ping" quando ICMP é excluído da transmissão IPsec por parte do computador. Além disso, uma vez que a resposta é

lenta durante a negociação inicial da chave, poderá demorar algum tempo a confirmar que a transmissão foi estabelecida.

Especificar Definições da chave de encriptação negociada automaticamente

Para alterar o método de autenticação do interlocutor da transmissão para as definições de código de encriptação negociado automaticamente para "Certificado", primeiro deve instalar e atribuir um certificado. Para mais informações sobre como criar e instalar um certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo". Para informações sobre o método de atribuição dos certificados instalados ao IPsec, consulte Pág. 134 "Selecionar o certificado para IPsec".

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [IPsec] sob "Segurança".**
4. **Clique em [Editar] sob "Definições da chave de encriptação negociada automaticamente".**
5. **Efetue as definições da chave de encriptação negociada automaticamente em [Definições 1].**

   Se pretender efetuar várias definições, selecione o número de definições e adicione as definições.
6. **Clique em [OK].**
7. **Selecione [Ativo] para " IPsec" em "IPsec".**
8. **Defina "Excluir comunicação HTTPS" para [Ativo] se não pretender utilizar o IPsec para transmissão HTTPS.**
9. **Clique em [OK].**
10. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

    Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
11. **Encerre sessão.**

Selecionar o certificado para IPsec

Utilizando o Web Image Monitor, selecione o certificado a ser utilizado para IPsec. É necessário instalar o certificado antes de poder ser utilizado. Para mais informações sobre como criar e instalar um certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo".

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**

2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o certificado a ser utilizado para IPsec na caixa em "IPsec", "Certificação".**
5. **Clique em [OK].**

   O certificado para IPsec é especificado.
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Especificar as definições IPsec do computador

Configure as definições IPsec do computador de modo a que correspondam exatamente ao nível de segurança do equipamento. Os métodos de definição diferem de acordo com o sistema operativo do computador. O procedimento de exemplo aqui apresentado utiliza o Windows 7 quando se encontra selecionado o nível de segurança de "Autenticação e baixa encriptação".

1. **No menu [Iniciar], clique em [Painel de Controlo], em [Sistema e Segurança] e, em seguida, clique em [Ferramentas Administrativas].**

   Com o Windows 8, passe o cursor sobre o canto superior ou inferior direito do ecrã e clique em [Definições], [Painel de controlo], [Sistema e segurança] e [Ferramentas administrativas].

   Se estiver a utilizar o Windows XP, no menu [Iniciar] clique em [Painel de Controlo], [Desempenho e Manutenção] e, em seguida, clique em [Ferramentas Administrativas].
2. **Clique duas vezes em [Política de segurança local].**

   Se aparecer a caixa de diálogo "Controlo da Conta do Utilizador", clique em [Sim].
3. **Clique em [Políticas de Segurança IP no Computador Local].**
4. **No menu "Ação", clique em [Criar Política de Segurança IP].**

   Aparece o Assistente da Política de Segurança IP.
5. **Clique em [Seguinte].**
6. **Introduza um nome para a política de segurança em "Nome" e clique em [Seguinte].**
7. **Retire a seleção da caixa de verificação "Ativar a regra de resposta predefinida" e clique em [Seguinte].**
8. **Selecione "Editar propriedades" e clique em [Terminar].**
9. **No separador "Geral", clique em [Definições].**

   Se utilizar o Windows XP, no separador "Geral", clique em [Avançadas].

10. **Em "Autenticar e gerar um novo código a cada", introduza o mesmo período de validade (em minutos) que é especificado no equipamento em "Definições da chave de encriptação negociada automaticamente, Fase 1" e, em seguida, clique em [Métodos].**
11. **Verifique se as definições do algoritmo hash ("Integridade"), algoritmo de encriptação ("Encriptação") e "Grupo Diffie-Helman" em "Ordem de preferência dos métodos de segurança" correspondem às especificadas no equipamento, em "Definições da chave de encriptação negociada automaticamente, Fase 1".**

    Se as definições não forem apresentadas, clique em [Adicionar].
12. **Clique duas vezes em [OK].**
13. **Clique em [Adicionar] no separador "Regras".**

    Aparece o Assistente de Regras de Segurança.
14. **Clique em [Seguinte].**
15. **Selecione "Esta regra não especifica um túnel" e clique em [Seguinte].**
16. **Selecione o tipo de rede para IPsec e clique em [Seguinte].**
17. **No Windows XP, selecione o método de autenticação e, em seguida, clique em [Seguinte]. No Windows 7/8, avance para o passo 18.**

    Se selecionar "Certificado" para o método de autenticação em "Definições da chave de encriptação negociada automaticamente" no equipamento, especifique a certificação do dispositivo. Se selecionar "PSK", introduza o mesmo texto PSK especificado no equipamento com o código pré-partilhado.
18. **Clique em [Adicionar] na Lista de Filtros IP.**
19. **Em [Nome], introduza um nome de Filtro IP e clique em [Adicionar].**

    Aparece o Assistente de Filtro IP.
20. **Clique em [Seguinte].**
21. **Se for necessário, introduza uma descrição do filtro IP e, em seguida, clique em [Seguinte].**

    No Windows XP, avance para o passo 22.
22. **Selecione "O Meu Endereço IP" em "Endereço de origem" e, em seguida, clique em [Seguinte].**
23. **Selecione "Um Endereço IP específico ou Subnet" em "Endereço de destino", introduza o endereço IP do equipamento e, em seguida, clique em [Seguinte].**

    Se utilizar o Windows XP, selecione "Um endereço IP específico" e clique em [Seguinte].
24. **Selecione o tipo de protocolo para IPsec e depois clique em [Seguinte].**

    Se utilizar IPsec com IPv6, selecione "58" como o número de protocolo para tipo de protocolo "Outro".
25. **Clique em [Concluir].**

26. **Clique em [OK].**
27. **Selecione o filtro IP acabado de criar e depois clique em [Seguinte].**
28. **Clique em [Adicionar].**

    É apresentado o assistente de ações de filtro.
29. **Clique em [Seguinte].**
30. **Em [Nome], introduza um nome de ação de filtro IP e, em seguida, clique em [Adicionar].**
31. **Selecione "Negociar segurança" e, em seguida, clique em [Seguinte].**
32. **Selecione "Permitir comunicação insegura se uma ligação segura não puder ser estabelecida." e, em seguida, clique em [Seguinte].**

    Se utilizar o Windows XP, selecione "Voltar à comunicação insegura" e clique em [Seguinte].
33. **Selecione "Personalizado" e clique em [Definições].**
34. **Em "Algoritmo de Integridade", selecione o algoritmo de autenticação que foi especificado no equipamento em "Definições da chave de encriptação negociada automaticamente, Fase 2".**
35. **Em "Algoritmo de Encriptação", selecione o algoritmo de encriptação que está especificado no equipamento em "Definições da chave de encriptação negociada automaticamente, Fase 2".**
36. **Nas "Definições dos códigos de sessão", selecione "Gerar um código novo a cada" e introduza o período de validade (em segundos) especificado no equipamento em "Definições da chave de encriptação negociada automaticamente, Fase 2".**
37. **Clique em [OK].**
38. **Clique em [Seguinte].**
39. **Clique em [Concluir].**
40. **Selecione a ação de filtro acabada de criar e, em seguida, clique em [Seguinte].**

    Se definir "Definições da chave de encriptação negociada automaticamente" para "Autenticação e elevada encriptação", selecione a ação do filtro IP acabada de criar, clique em [Editar] e assinale "Utilizar a chave de Perfect Forward Secrecy (PFS)" na caixa de diálogo das propriedades do filtro. Se utilizar PFS no Windows XP, o número de grupo PFS utilizado na fase 2 é negociado automaticamente na fase 1 a partir do número de grupo Diffie-Hellman (definido no passo 11). Consequentemente, se alterar as definições automáticas especificadas do nível de segurança no equipamento e aparecer "Definição do utilizador", deve definir o mesmo número de grupo para a "Fase 1 do Grupo Diffie-Hellman" e "Fase 2 PFS" no equipamento para estabelecer a transmissão IPsec.

41. **Selecione o método de autenticação e, em seguida, clique em [Seguinte]. No Windows XP, avance para o passo 42.**

    Se selecionar "Certificado" para o método de autenticação em "Definições da chave de encriptação negociada automaticamente" no equipamento, especifique a certificação do dispositivo. Se selecionar "PSK", introduza o mesmo texto PSK especificado no equipamento com o código pré-partilhado.

42. **Clique em [Concluir].**

43. **Clique em [OK].**

    Se utilizar o Windows XP, clique em [Fechar].

    A nova política de segurança IP (definições IPsec) está especificada.

44. **Selecione a política de segurança acabada de criar, faça clique com o botão direito do rato e clique em [Atribuir].**

    As definições IPsec do computador são ativadas.

Nota

- Para desativar as definições IPsec do computador, selecione a política de segurança, faça clique com o botão direito do rato e, em seguida, clique em [Retirar atribuição].

Comandos de definição telnet

É possível utilizar telnet para confirmar as definições IPsec e efetuar alterações às definições. Esta secção explica os comandos telnet para IPsec. Para mais informações sobre o nome de utilizador e palavra-passe de início de sessão no telnet, contacte o administrador. Para detalhes sobre como iniciar sessão em telnet e operações telnet, consulte Connecting the Machine/ System Settings.

Importante

- **Se utilizar um certificado como método de autenticação nas definições de chave de encriptação negociada automaticamente (IKE), instale o certificado utilizando o Web Image Monitor. Não é possível instalar um certificado utilizando telnet.**

ipsec

Para visualizar informações de definições relacionadas com IPsec, utilize o comando "ipsec".

Visualizar definições atuais

```
msh> ipsec
```

Apresenta as seguintes informações sobre definições IPsec:

- Valores das definições de IPsec
- Definições manuais da chave de encriptação, valores de definição IKE 1-4

- Definições manuais da chave de encriptação, valores predefinidos IKE

Apresentar as partes de definições atuais

```
msh> ipsec -p
```

- Apresenta as informações sobre definições IPsec em partes.

ipsec exclude

Para visualizar ou especificar os protocolos excluídos por IPsec, utilize o comando "ipsec exclude".

Visualizar definições atuais

```
msh> ipsec exclude
```

- Apresenta os protocolos atualmente excluídos da transmissão IPsec.

Especificar os protocolos a excluir

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Especifique o protocolo e introduza [on] para o excluir ou [off] para o incluir na transmissão IPsec. Se introduzir [all], todos os protocolos são especificados em conjunto.

ipsec ike

Para visualizar ou especificar as definições de código de encriptação negociado automaticamente, utilize o comando "ipsec ike".

Visualizar definições atuais

```
msh> ipsec ike {1|2|3|4|default}
```

- Para visualizar as definições 1-4, especifique o número [1-4].
- Para visualizar a predefinição, especifique [default].
- Não especificar nenhum valor apresenta todas as definições.

Desativar definições

```
msh> ipsec ike {1|2|3|4|default} disable
```

- Para desativar as definições 1-4, especifique o número [1-4].
- Para desativar as predefinições, especifique [default].

Especifique o endereço local/endereço remoto do utilizador.

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Introduza o número da definição individual [1-4] e o tipo de endereço para especificar o endereço local e remoto.
- Para definir os valores de endereço local ou remoto, especifique masklen introduzindo [/] e um número inteiro de 0 a 32 aquando da definição de um endereço IPv4. Na definição de um endereço IPv6, especifique masklen introduzindo [/] e um número inteiro de 0 a 128.

- Não especificar nenhum valor de endereço apresenta a definição atual.

Especificar o tipo de endereço na predefinição

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Especifique o tipo de endereço para a predefinição.
- Para especificar IPv4 e IPv6, introduza [any].

Definição da política de segurança

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique a política de segurança para o endereço especificado na definição selecionada.
- Para aplicar IPsec aos pacotes relevantes, especifique [apply]. Para não aplicar IPsec, especifique [bypass].
- Se especificar [discard], são descartados todos os pacotes aos quais seja possível aplicar o IPsec.
- Não especificar uma política de segurança apresenta a definição atual.

Definição do protocolo de segurança

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o protocolo de segurança.
- Para especificar AH, introduza [ah]. Para especificar ESP, introduza [esp]. Para especificar AH e ESP, introduza [dual].
- Não especificar um protocolo apresenta a definição atual.

Definição do nível de requisito IPsec

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o nível de requisito IPsec.
- Se especificar [require], os dados não serão transmitidos se não for possível utilizar o IPsec. Se especificar [use], os dados serão enviados normalmente se não for possível utilizar o IPsec. Quando for possível utilizar IPsec, é executada a transmissão IPsec.
- Não especificar um requisito de nível apresenta a definição atual.

Definição do modo de encapsulamento

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o modo de encapsulamento.
- Para especificar o modo de transporte, introduza [transport]. Para especificar o modo de túnel, introduza [tunnel].

- Se tiver definido o tipo de endereço na predefinição para [any], não é possível utilizar [tunnel] no modo de encapsulamento.
- Não especificar um modo de encapsulamento apresenta a definição atual.

Definição de túnel e ponto de fim

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP address"
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o endereço IP de início e de fim do ponto de fim de túnel.
- Não especificar o endereço de início ou fim apresenta a definição atual.

Definição do método de autenticação do interlocutor IKE

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o método de autenticação.
- Especifique [psk] para utilizar uma chave partilhada como método de autenticação. Especifique [rsasig] para utilizar um certificado como método de autenticação.
- Se selecionar [psk], é também necessário especificar a cadeia de carateres PSK.
- Note que se selecionar "Certificado", é necessário instalar e especificar o certificado para IPsec antes de poder utilizá-lo. Para instalar e especificar o certificado utilize o Web Image Monitor.

Definição da cadeia de carateres PSK

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- Se selecionar PSK como método de autenticação, introduza o número da definição individual [1-4] ou [default] e especifique a cadeia de carateres PSK.
- Especifique a cadeia de carateres ASCII. Não são permitidas abreviaturas.

Definição do algoritmo hash de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo hash de SA ISAKMP (fase 1).
- Não especificar o algoritmo hash apresenta a definição atual.

Definição do algoritmo de encriptação de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de encriptação de SA ISAKMP (fase 1).
- Não especificar um algoritmo de encriptação apresenta a definição atual.

Definição do grupo Diffie-Hellman de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o número do grupo Diffie-Hellman de SA ISAKMP (fase 1).
- Especifique o número de grupo a ser utilizado.
- Não especificar um número de grupo apresenta a definição atual.

Definição do período de validade de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o período de validade de SA ISAKMP (fase 1).
- Introduza o período de validade (em segundos) de 300 a 172 800.
- Não especificar um período de validade apresenta a definição atual.

Definição do algoritmo de autenticação de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-
-sha384|hmac-sha512}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de autenticação de SA IPsec (fase 2).
- Separe as entradas de vários algoritmos de encriptação com uma vírgula (,). Os valores de definição atuais são apresentados pela ordem de maior prioridade.
- Não especificar um algoritmo de autenticação apresenta a definição atual.

Definição do algoritmo de encriptação de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|
aes256}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de encriptação de SA IPsec (fase 2).
- Separe as entradas de vários algoritmos de encriptação com uma vírgula (,). Os valores de definição atuais são apresentados pela ordem de maior prioridade.
- Não especificar um algoritmo de encriptação apresenta a definição atual.

Definição PFS de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o número do grupo Diffie-Hellman de SA IPsec (fase 2).
- Especifique o número de grupo a ser utilizado.
- Não especificar um número de grupo apresenta a definição atual.

Definição do período de validade de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o período de validade de SA IPsec (fase 2).

- Introduza o período de validade (em segundos) de 300 a 172 800.
- Não especificar um período de validade apresenta a definição atual.

Repor os valores de definição

```
msh> ipsec ike {1|2|3|4|default|all} clear
```

- Introduza o número da definição individual [1-4] ou [default] e reponha a definição especificada. A especificação de [all] repõe todas as definições, incluindo as predefinições.

Configurar a Autenticação IEEE 802.1X

IEEE 802.1X é um standard de autenticação e utiliza o servidor de autenticação (servidor RADIUS). Pode ser utilizado em redes com e sem fios.

É possível selecionar 4 tipos de método de autenticação EAP: EAP-TLS, LEAP, EAP-TTLS e PEAP. Tenha em atenção que cada método de autenticação EAP tem diferentes definições de configuração e procedimentos de autenticação.

Os tipos e os requisitos relativos às certificações são os seguintes:

Tipo EAP	Certificações necessárias
EAP-TLS	Certificado externo, Certificado do dispositivo (Certificado de cliente IEEE 802.1X)
LEAP	-
EAP-TTLS	Certificado externo
PEAP	Certificado externo
PEAP (a Fase 2 é apenas para TLS)	Certificado externo, Certificado do dispositivo (Certificado de cliente IEEE 802.1X)

Instalar um certificado externo

Instale um certificado externo (certificado root CA) para verificar a fiabilidade do servidor de autenticação. É necessário possuir, pelo menos, um certificado emitido pela autoridade de certificação que assinou o certificado do servidor ou um certificado de uma autoridade de certificação superior.

Apenas podem ser importados certificados de web site PEM (X.509 com codificação Base64).

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado externo] sob "Segurança".**
4. **Clique [Procurar] para "Certificado externo a importar" e, em seguida, selecione o certificado CA obtido.**
5. **Clique em [Abrir].**
6. **Clique em [Importar].**
7. **Verifique se o [Estado] do certificado importado indica "Fidedigno".**

   Se [Verificar certificado a partir do site] estiver no modo [Ativo] e o [Estado] do certificado for [Não fidedigno], a comunicação pode não ser possível.

8. **Clique em [OK].**
9. **Encerre sessão.**

Selecionar o certificado do dispositivo

Selecione o certificado que pretende utilizar com IEEE 802.1X de entre os certificados de dispositivo que foram criados e instalados previamente no equipamento. Para mais informações sobre como criar e instalar um certificado do dispositivo, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo".

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Certificado do dispositivo] sob "Segurança".**
4. **Selecione o certificado a ser utilizado para IEEE 802.1X na caixa em "IEEE 802.1X","Certificação".**
5. **Clique em [OK].**
6. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
7. **Encerre sessão.**

Itens de definição de IEEE 802.1X para Ethernet

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [IEEE 802.1X] sob "Segurança".**
4. **Em "Nome de utilizador", introduza o nome de utilizador definido no servidor RADIUS.**
5. **Introduza o nome de domínio em "Nome de domínio".**
6. **Selecione "Tipo EAP". As configurações diferem de acordo com o Tipo EAP.**

   EAP-TLS

   - Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
     - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
     - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
     - Introduza o nome de host do servidor RADIUS em "ID de servidor".
     - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

LEAP

- Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.

EAP-TTLS

- Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.
- Clique em [Alterar] em "Nome de utilizador da fase 2" e, em seguida, introduza o nome de utilizador definido no servidor RADIUS.
- Selecione [CHAP], [MSCHAP], [MSCHAPv2], [PAP] ou [MD5] em "Método da fase 2".

  Pode dar-se o caso de certos métodos não estarem disponíveis, dependendo do servidor RADIUS que pretende utilizar.
- Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
  - Introduza o nome de host do servidor RADIUS em "ID de servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

PEAP

- Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.

  Se for selecionado [TLS] para "Método da fase 2", não precisa de especificar uma palavra--passe.
- Clique em [Alterar] em "Nome de utilizador da fase 2" e, em seguida, introduza o nome de utilizador definido no servidor RADIUS.
- Selecione [MSCHAPv2] ou [TLS] em"Método da fase 2".

  Quando selecionar [TLS], tem de instalar "Certificado de cliente IEEE 802.1X".
- Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
  - Introduza o nome de host do servidor RADIUS em "ID de servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

7. **Clique em [OK].**
8. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.

9. **Clique em [Definições do interface] sob "Interface".**
10. **Selecione [Ativo] em "Segurança Ethernet".**
11. **Clique em [OK].**
12. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

    Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
13. **Encerre sessão.**

Nota

- Se ocorrer um problema com as definições, poderá não ser possível comunicar com o equipamento. Neste caso, aceda a [Imprimir lista] em [Definições interface] no painel de controlo e, em seguida, imprima o resumo de rede para verificar o estado.
- Se não for possível identificar o problema, execute [Repor predefinições da autenticação IEEE 802.1X] em [Rede] nas [Definições interface] no painel de controlo e repita o procedimento.

Itens de definição de IEEE 802.1X para Wireless LAN

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [IEEE 802.1X] sob "Segurança".**
4. **Em "Nome de utilizador", introduza o nome de utilizador definido no servidor RADIUS.**
5. **Introduza o nome de domínio em "Nome de domínio".**
6. **Selecione "Tipo EAP". As configurações diferem de acordo com o Tipo EAP.**

   EAP-TLS

   - Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
     - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
     - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
     - Introduza o nome de host do servidor RADIUS em "ID de servidor".
     - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

   LEAP

   - Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.

   EAP-TTLS

   - Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.

- Clique em [Alterar] em "Nome de utilizador da fase 2" e, em seguida, introduza o nome de utilizador definido no servidor RADIUS.
- Selecione [CHAP], [MSCHAP], [MSCHAPv2], [PAP] ou [MD5] em "Método da fase 2".

  Pode dar-se o caso de certos métodos não estarem disponíveis, dependendo do servidor RADIUS que pretende utilizar.
- Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
  - Introduza o nome de host do servidor RADIUS em "ID de servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

PEAP

- Clique em [Alterar] em "Palavra-passe" e, em seguida, introduza a palavra-passe definida no servidor RADIUS.

  Se for selecionado [TLS] para "Método da fase 2", não precisa de especificar uma palavra--passe.
- Clique em [Alterar] em "Nome de utilizador da fase 2" e, em seguida, introduza o nome de utilizador definido no servidor RADIUS.
- Selecione [MSCHAPv2] ou [TLS] em"Método da fase 2".

  Quando selecionar [TLS], tem de instalar "Certificado de cliente IEEE 802.1X".
- Execute as seguintes definições, de acordo com o sistema operativo que utilizar:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Aceitar autoridade de certificação intermédia".
  - Introduza o nome de host do servidor RADIUS em "ID de servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

7. **Clique em [OK].**
8. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
9. **Clique em [Definições de wireless LAN] sob "Interface".**
10. **Selecione [Wireless LAN] em "Tipo de rede".**
11. **Selecione o [Modo de infraestrutura] no "Modo de comunicação".**
12. **Introduza os carateres alfanuméricos (a-z, A-Z, ou 0-9) em [SSID] de acordo com o ponto de acesso que pretende utilizar.**
13. **Selecione [WPA2] em "Método de segurança".**

14. **Selecione [WPA2] em "Método de autenticação WPA2".**
15. **Clique em [OK].**
16. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

    Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
17. **Encerre sessão.**

Nota

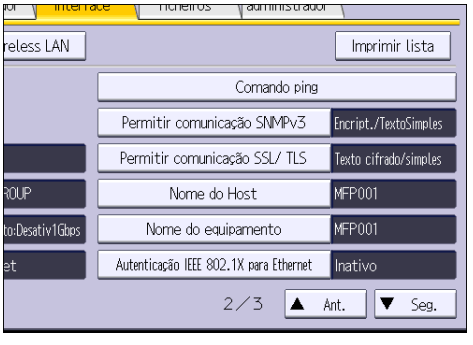
- Se ocorrer um problema com as definições, poderá não ser possível comunicar com o equipamento. Neste caso, aceda a [Imprimir lista] em [Definições interface] no painel de controlo e, em seguida, imprima o resumo de rede para verificar o estado.
- Se não for possível identificar o problema, execute [Repor predefinições da autenticação IEEE 802.1X] em [Rede] nas [Definições interface] no painel de controlo e repita o procedimento.

Encriptação SNMPv3

Ao utilizar o Device Manager NX ou outra aplicação que comunique via SNMPv3, é possível encriptar os dados transmitidos.

Efetuando esta definição, pode proteger os dados de manipulação.

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Defin. interface].**
4. **Prima [▼Seg.].**
5. **Prima [Permitir comunicação SNMPv3].**



6. **Prima [Só encriptação].**
7. **Prima [OK].**
8. **Encerre sessão.**

Nota

- Para usar o Device Manager NX para encriptar os dados de especificação de definições, é necessário especificar a definição [Palavra-passe de encriptação] do administrador de rede e [Encrypted Password] em [SNMP Account Setting] do Device Manager NX, além de especificar [Permitir comunicação SNMPv3] no equipamento. Para detalhes sobre como especificar a [Encrypted Password] no Device Manager NX, consulte a Ajuda do Device Manager NX.
- Se a definição da [Pal.-passe de encriptação] do administrador da rede não estiver especificada, os dados para transmissão podem não ser encriptados ou enviados. Para mais informações sobre como especificar a definição [Pal.-passe de encriptação] do administrador da rede, consulte Pág. 16 "Registar e alterar administradores".

Encriptar Palavras-Passe Transmitidas

Configurar o código de encriptação do driver e a encriptação de palavra-passe para autenticação IPP permite as comunicações com palavras-passe encriptadas, além de aumentar a segurança das palavras-passe contra a descodificação. Para aumentar ainda mais a segurança, recomendamos a utilização de IPsec, SNMPv3 e SSL/TLS em conjunto.

Encripte também as palavras-passe para autenticação do administrador e dos utilizadores.

Código de encriptação do controlador

Esta chave é uma cadeia de carateres utilizada para encriptar as palavras-passe de início de sessão enviadas de cada driver quando a autenticação de utilizador está ativada.

Para encriptar a palavra-passe de início de sessão, especifique o código de encriptação do driver no equipamento e no driver da impressora instalado no computador do utilizador.

Palavra-passe para Autenticação IPP

Para encriptar a palavra-passe de Autenticação IPP no Web Image Monitor, defina "Autenticação" para [DIGEST] e especifique a palavra-passe de autenticação IPP no equipamento.

Pode utilizar Telnet ou FTP para gerir palavras-passe para a autenticação IPP, embora não seja recomendado.

Nota

- Para mais informações sobre como encriptar as palavras-passe de início de sessão para autenticação do administrador, consulte Pág. 16 "Registar e alterar administradores".

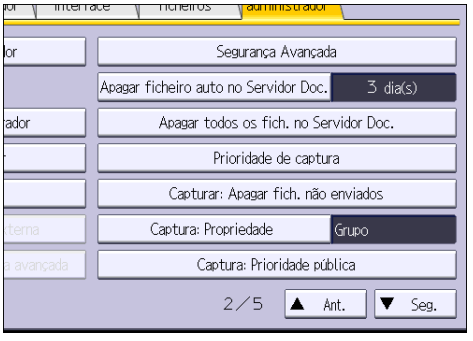
Especificar um código de encriptação do controlador

Especifique a chave de encriptação do driver no equipamento.

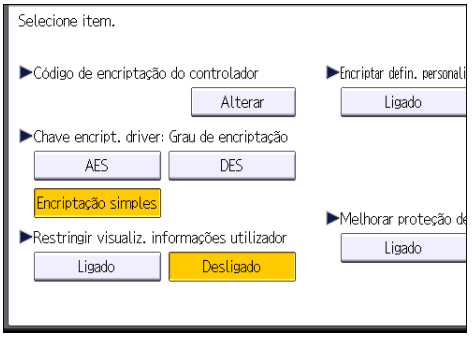
Esta definição ativa a transmissão encriptada de palavras-passe de início de sessão e reforça a segurança contra a descodificação de palavras-passe.

1. **Inicie sessão como administrador de rede no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**

5. **Prima [Segurança Avançada].**



6. **Para o "Código de encriptação do controlador", prima em [Alterar].**



7. **Introduza o código de encriptação do driver e, em seguida, prima [OK].**

   Introduza a chave de encriptação do driver utilizando até 32 carateres alfanuméricos.

   O administrador da rede deve fornecer aos utilizadores o código de encriptação do controlador especificado no equipamento para que o possam registar nos seus computadores. Certifique-se de que introduz o mesmo código de encriptação do driver que está especificado no equipamento.

8. **Prima [OK].**

9. **Encerre sessão.**

Nota

- Para detalhes sobre como especificar a chave de encriptação no driver de impressão ou driver TWAIN, consulte a ajuda do driver.

Especificar uma palavra-passe de Autenticação IPP

Especifique uma palavra-passe de autenticação de IPP para este equipamento. Esta definição ativa a transmissão encriptada de palavras-passe de autenticação IPP e reforça a segurança contra a descodificação de palavras-passe.

1. **Inicie sessão como administrador de rede a partir do Web Image Monitor.**

2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Autenticação IPP] sob "Segurança".**
4. **Selecione [DIGEST] da lista "Autenticação".**
5. **Introduza o nome de utilizador na caixa "Nome de utilizador".**
6. **Introduza a palavra-passe na caixa "Palavra-passe".**
7. **Clique em [OK].**

   A autenticação IPP está especificada.
8. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.
9. **Encerre sessão.**

Definição da Encriptação de Autenticação Kerberos

É possível especificar a transmissão encriptada entre o equipamento e o servidor KDC quando a autenticação Kerberos está ativada.

A utilização da autenticação Kerberos com a autenticação Windows, autenticação LDAP ou busca LDAP garante uma comunicação segura.

O algoritmo de encriptação suportado difere conforme o tipo de servidor KDC. Selecione o algoritmo que melhor se adequa ao seu ambiente.

Servidor KDC	Algoritmos de encriptação suportados
Windows Server 2003 Active Directory	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* Para a autenticação Kerberos poder ser utilizada, ative-a nas definições do sistema operativo.

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Autenticação Kerberos] sob "Definições do dispositivo".**
4. **Selecione o algoritmo de encriptação que pretende ativar.**

   Certifique-se de que seleciona um ou mais algoritmos de encriptação.

5. Clique em [OK].
6. Encerre sessão.

6. Prevenir Contra a Fuga de Documentos

Este capítulo explica como proteger os dados dos documentos guardados no equipamento ou impressos utilizando o equipamento.

Gerir Pastas

Esta secção explica como gerir as pastas no servidor de documentos, como eliminar pastas, alterar as respetivas palavras-passes e desbloqueá-las quando estão bloqueadas.

Eliminar pastas

Pode ser feito pelo administrador de ficheiros ou por um utilizador.

Para eliminar uma pasta com o ícone ao lado, é necessária a palavra-passe da pasta.

No caso de um utilizador se esquecer da palavra-passe de acesso à pasta, o administrador de ficheiros pode alterá-la.

O administrador de ficheiros pode eliminar pastas sem utilizar a palavra-passe.

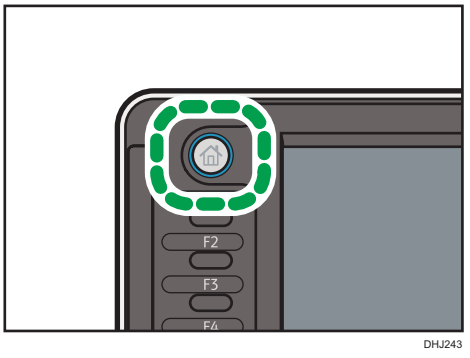
Não podem ser eliminadas pastas que contêm ficheiros que o utilizador não tem permissão para eliminar.

Não é possível eliminar a pasta partilhada.

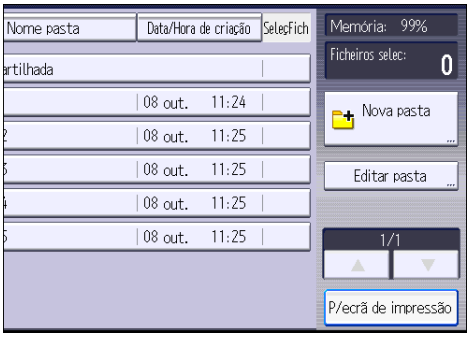
1. **Inicie sessão como administrador de ficheiros ou utilizador no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].



4. **Prima [Editar pasta].**



5. **Selecione a pasta.**
6. **Prima [Apagar].**
7. **Se surgir o ecrã de introdução da palavra-passe, introduza a palavra-passe da pasta e prima [OK].**

   O ecrã de entrada da palavra-passe não aparece se o administrador de ficheiros tiver iniciado sessão.
8. **Prima [Apagar].**
9. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Alterar a palavra-passe de uma pasta

Isto pode ser especificado pelo administrador de ficheiros ou por um utilizador.

No caso de um utilizador se esquecer da palavra-passe de acesso à pasta, o administrador de ficheiros pode alterá-la.

Não é possível especificar uma palavra-passe para a pasta partilhada.

1. **Inicie sessão como administrador de ficheiros ou utilizador no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
4. **Prima [Editar pasta].**
5. **Selecione a pasta.**
6. **Prima [Alt. palavra-passe].**
7. **Se surgir o ecrã de introdução da palavra-passe, introduza a palavra-passe da pasta e prima [OK].**

   O ecrã de entrada da palavra-passe não aparece se o administrador de ficheiros tiver iniciado sessão.
8. **Introduza a nova palavra-passe para a pasta e prima [OK].**

   Pode utilizar 4 a 8 números como palavra-passe para a pasta.
9. **Introduza a palavra-passe de confirmação novamente e, em seguida, prima [OK].**

   O ícone surge ao lado de uma pasta protegida por palavra-passe.
10. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Desbloquear pastas

Só o administrador de ficheiros pode desbloquear pastas.

Se especificar [Ligado] para "Melhorar proteção de ficheiros", a pasta será bloqueada e ficará inacessível se for introduzida 10 vezes uma palavra-passe inválida. Este capítulo explica como desbloquear pastas.

"Melhorar proteção de ficheiros" é uma das funções de segurança avançadas. Para mais informações sobre esta e outras funções de segurança avançadas, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".

1. **Inicie sessão como administrador de ficheiros no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador].**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

4. **Prima [Editar pasta].**
5. **Selecione a pasta.**

   O ícone surge ao lado de uma pasta bloqueada pela função Melhorar proteção de ficheiros.

6. **Prima [Desbloquear].**

   O ícone muda para o ícone .

7. **Prima [Desbloquear].**
8. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Gerir Ficheiros Guardados

Esta secção descreve como especificar as permissões de acesso a ficheiros guardados.

Pode especificar a quem é permitido o acesso a ficheiros digitalizados guardados e a ficheiros guardados no Servidor de documentos.

Assim evita atividades como a impressão ou o envio de ficheiros guardados por utilizadores não autorizados.

Também pode especificar os utilizadores que podem alterar ou apagar ficheiros guardados.

Para limitar a utilização de ficheiros guardados, pode especificar 4 tipos de permissões de acesso.

Tipo de permissão de acesso

Permissão de acesso	Descrição
Só de leitura	Pode verificar o conteúdo de e as informações sobre ficheiros guardados, imprimir e enviar os ficheiros.
Editar	Pode alterar as definições de impressão para ficheiros guardados. Isto inclui a permissão para visualizar ficheiros.
Editar/ Apagar	Pode apagar ficheiros guardados. Isto inclui a permissão para visualizar e editar ficheiros.
Controlo total	Pode especificar o utilizador e a permissão de acesso. Isto inclui a permissão para visualizar, editar e editar/apagar ficheiros.

Palavra-passe para ficheiros guardados

- As palavras-passes para ficheiros guardados podem ser especificadas pelo administrador de ficheiros ou proprietário. Pode aumentar a proteção contra a utilização não autorizada de ficheiros. Para mais informações sobre como atribuir uma palavra-passe a um ficheiro guardado, consulte Pág. 167 "Especificar palavras-passe para ficheiros guardados".
- Mesmo que a autenticação de utilizador não esteja definida, podem ser definidas palavras--passe para os ficheiros guardados.

Nota

- Os ficheiros podem ser guardados por qualquer utilizador que tenha autorização para utilizar o servidor de documentos, a função de cópia, a função de scanner ou a função de impressão.
- Utilizando o Web Image Monitor, pode verificar o conteúdo de ficheiros guardados. Para mais informações, consulte a Ajuda do Web Image Monitor.

- A permissão de acesso predefinida para o proprietário é "Só de leitura". Também pode especificar a permissão de acesso.
- O administrador de ficheiros não só configura as permissões de acesso como também pode eliminar os ficheiros guardados. Para mais informações sobre os métodos de eliminação de documentos, consulte Copy/ Document Server.

Configurar permissões de acesso para cada ficheiro guardado

Esta opção pode ser especificada pelo administrador de ficheiros ou proprietário.

Especifique os utilizadores e as suas permissões de acesso para cada ficheiro guardado.

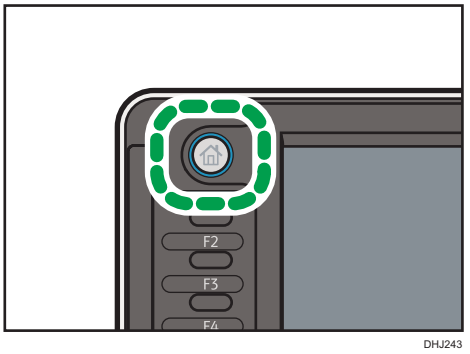
Importante

- **Se os ficheiros ficarem inacessíveis, restabeleça a permissão de acesso aos mesmos na qualidade de proprietário. O administrador de ficheiros pode restabelecer a permissão de acesso. Se pretende aceder a um ficheiro, mas não tem permissão de acesso, peça ao proprietário.**
- **O administrador de ficheiros pode alterar o proprietário de um documento utilizando a definição [Alt. privil. acesso]. Esta definição permite também ao administrador de ficheiros alterar os privilégios de acesso do proprietário e outros utilizadores.**
- **O proprietário do documento e os utilizadores com o privilégio de [Controlo total] sobre o documento podem alterar os privilégios de acesso do proprietário e dos outros utilizadores na definição [Alt. privil. acesso].**

1. **Inicie sessão como administrador de ficheiros ou proprietário no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

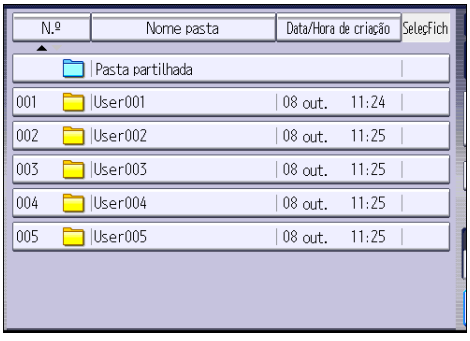
   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

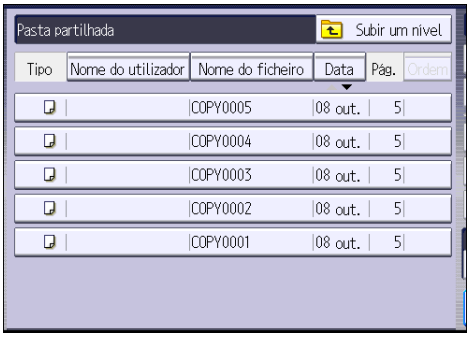


DHJ243

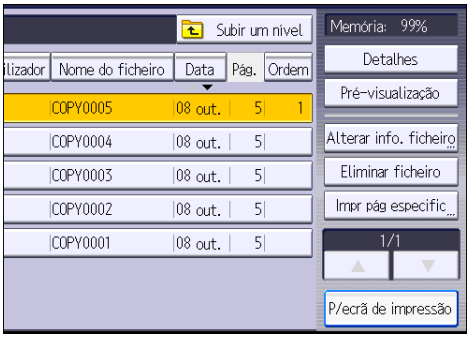
4. Selecione a pasta.



5. Selecione o ficheiro.



6. Prima [Alterar info. ficheiro].

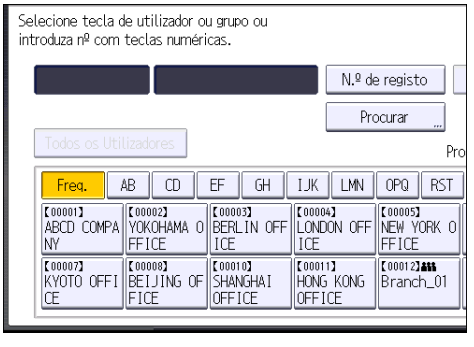


7. Prima [Alt. privil. acesso].

8. **Prima [Programar/Alt./Apagar].**



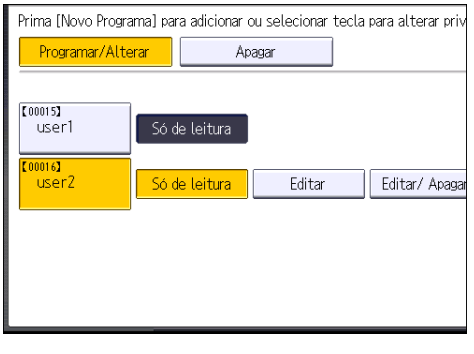
9. **Prima [Novo programa].**
10. **Selecione os utilizadores ou grupos aos quais deseja atribuir permissões de acesso.**



Pode selecionar vários utilizadores.

Se premir [Todos os Utilizadores], pode selecionar todos os utilizadores.

11. **Prima [Sair].**
12. **Selecione o utilizador a quem pretende atribuir uma permissão de acesso, selecionando depois a permissão.**



Selecione a permissão, a partir de [Só de leitura], [Editar], [Editar/ Apagar] ou [Controlo total].

13. **Prima [Sair].**
14. **Prima [OK].**

15. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- As permissões de acesso "Editar", "Editar/ Apagar" e "Controlo total" permitem ao utilizador executar operações de alto nível que podem resultar na perda de ou em alterações em informações delicadas. Recomendamos que apenas atribua a permissão "Só de leitura" à generalidade dos utilizadores.

Alterar o proprietário de um documento

Utilize este procedimento para alterar o proprietário de um documento.

Apenas o administrador de ficheiros pode alterar o proprietário de um documento.

1. **Inicie sessão como administrador de ficheiros no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
4. **Selecione a pasta.**
5. **Selecione o ficheiro.**
6. **Prima [Alterar info. ficheiro].**
7. **Prima [Alt. privil. acesso].**
8. **Prima [Alterar] para "Proprietário".**
9. **Selecione o utilizador que pretende registar.**
10. **Prima [Sair].**
11. **Prima [OK].**
12. **Encerre sessão.**

Configurar as permissões de acesso para cada utilizador referentes a ficheiros guardados

Isto pode ser especificado pelo administrador de utilizadores ou proprietário.

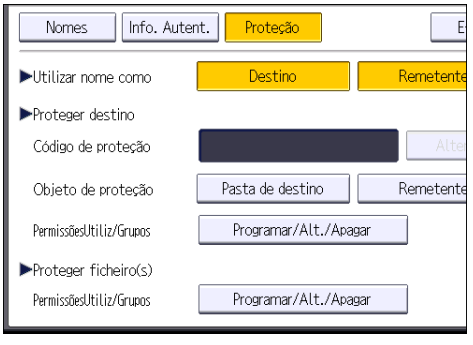
Especifique os utilizadores e a sua permissão de acesso a ficheiros guardados por um determinado utilizador.

Isto torna a gestão de permissão de acesso mais fácil do que especificar e gerir permissões de acesso para cada ficheiro guardado.

Importante

- **Se os ficheiros ficarem inacessíveis, certifique-se de que solicita ao administrador de utilizadores que restabeleça as permissões de acesso aos ficheiros.**

1. **O administrador de utilizadores ou o proprietário inicia sessão no painel de controlo.**
2. **Prima [Gestão livro de endereços].**
3. **Selecione o utilizador.**
4. **Prima [Proteção].**
5. **Em "Proteger ficheiro(s)", prima [Programar/Alt./Apagar] para "PermissõesUtiliz/Grupos".**

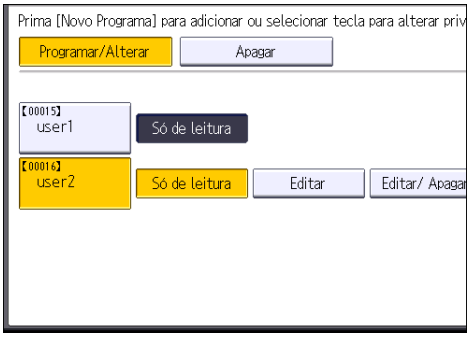


6. **Prima [Novo programa].**
7. **Selecione os utilizadores ou os grupos a registar.**

   Pode selecionar vários utilizadores.

   Se premir [Todos os Utilizadores], pode selecionar todos os utilizadores.
8. **Prima [Sair].**

9. **Selecione o utilizador a quem pretende atribuir uma permissão de acesso, selecionando depois a permissão.**



   Selecione a permissão, a partir de [Só de leitura], [Editar], [Editar/ Apagar] ou [Controlo total].

10. **Prima [Sair].**
11. **Prima [OK].**
12. **Prima [Sair].**
13. **Encerre sessão.**

Nota

- As permissões de acesso "Editar", "Editar/ Apagar" e "Controlo total" permitem ao utilizador executar operações de alto nível que podem resultar na perda de ou em alterações em informações delicadas. Recomendamos que apenas atribua a permissão "Só de leitura" à generalidade dos utilizadores.

Especificar palavras-passe para ficheiros guardados

Esta opção pode ser especificada pelo administrador de ficheiros ou proprietário.

1. **O administrador de ficheiros ou o proprietário inicia sessão no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

4. **Selecione a pasta.**
5. **Selecione o ficheiro.**

6. **Prima [Alterar info. ficheiro].**



7. **Prima [Alt. palavra-passe].**
8. **Introduza a nova palavra-passe para o ficheiro guardado e, em seguida, prima [OK].**

   Pode utilizar 4 a 8 números como a palavra-passe para o ficheiro guardado.
9. **Introduza novamente a palavra-passe para fins de confirmação e, em seguida, prima [OK].**

   O ícone surge ao lado de um ficheiro guardado protegido por palavra-passe.
10. **Prima [OK].**
11. **Encerre sessão.**

Desbloquear ficheiros guardados

Só o administrador de ficheiros pode desbloquear ficheiros.

Se especificar "Melhorar proteção de ficheiros", o ficheiro será bloqueado e torna-se inacessível se uma palavra-passe inválida for introduzida 10 vezes. Este capítulo explica como desbloquear ficheiros.

"Melhorar proteção de ficheiros" é uma das funções de segurança avançadas. Para mais informações sobre esta e outras funções de segurança avançadas, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".

1. **Inicie sessão como administrador de ficheiros no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e, em seguida, prima o ícone [Servidor de documentos] no ecrã.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
4. **Selecione a pasta.**

5. **Selecione o ficheiro.**

   O ícone surge ao lado de ficheiros bloquados pela função Melhorar proteção de ficheiros.

6. **Prima [Alterar info. ficheiro].**

7. **Prima [Desbloq. ficheiros].**



8. **Prima [Sim].**

   O ícone muda para o ícone .

9. **Prima [OK].**

10. **Encerre sessão.**

Gerir Ficheiros de Impressão Bloqueada

Dependendo da localização do equipamento, poderá ser difícil evitar que pessoas não autorizadas vejam as impressões carregadas nas bandejas de saída. Quando imprimir documentos confidenciais, utilize a função Impressão Bloqueada.

Impressão bloqueada

- Utilizando a função da impressora Impressão bloqueada, pode guardar ficheiros no equipamento como ficheiros de Impressão bloqueada. Em seguida, imprima os ficheiros a partir do painel de controlo e recupere-os de imediato para que os outros não os vejam.

Nota

- É possível imprimir documentos confidenciais independentemente das definições de autenticação do utilizador.
- Para guardar ficheiros temporariamente, selecione [Impressão guardada] no driver de impressão. Se selecionar [Impressão guardada (Partilhada)], também pode partilhar estes ficheiros.
- Para mais informações sobre como utilizar a função de Impressão bloqueada, consulte Print.

Eliminar ficheiros de impressão bloqueada

Esta opção pode ser especificada pelo administrador de ficheiros ou proprietário.

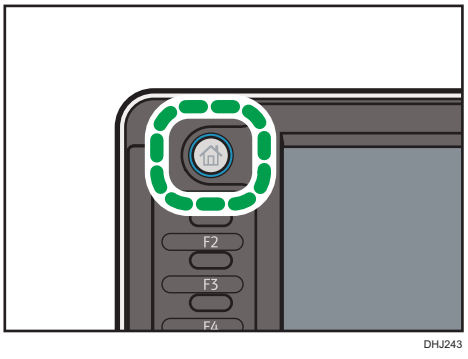
Para o proprietário poder eliminar um ficheiro de impressão bloqueada, é necessária a palavra-passe de acesso ao ficheiro. Se o proprietário se esqueceu da palavra-passe, o administrador de ficheiros pode alterá-la.

O administrador de ficheiros não necessita da palavra-passe para eliminar ficheiros de impressão bloqueada.

1. **Inicie sessão como administrador de ficheiros ou proprietário no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

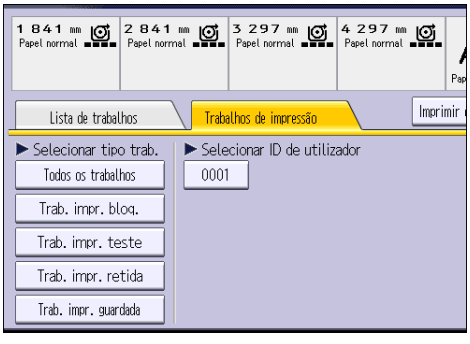
   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

3. Prima a tecla [Ecrã inicial] no painel de controlo e prima o ícone [Impressora] no ecrã.

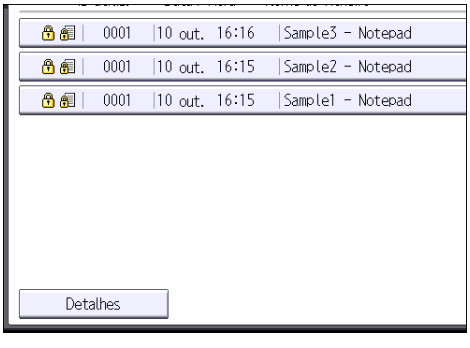


DHJ243

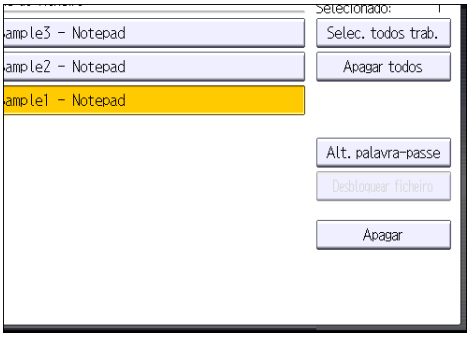
4. Prima [Trabalhos de impressão].
5. Prima [Trab. impr. bloq.].



6. Selecione o ficheiro.



7. **Prima [Apagar].**



8. **Se aparecer um ecrã para introdução da palavra-passe, introduza a palavra-passe do ficheiro de impressão bloqueada e, em seguida, prima [OK].**

   O ecrã de entrada da palavra-passe não aparece se o administrador de ficheiros tiver iniciado sessão.

9. **Prima [Sim].**
10. **Encerre sessão.**

Nota

- Pode configurar este equipamento para apagar ficheiros guardados automaticamente definindo a opção "Apagar auto trab. de impressão temporários" como [Ligado]. Para mais informações sobre "Apagar auto trab. de impressão temporários", consulte Print.
- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Alterar a palavra-passe de um ficheiro de impressão bloqueada

Esta opção pode ser especificada pelo administrador de ficheiros ou proprietário.

Se o proprietário se esqueceu da palavra-passe, o administrador de ficheiros pode alterá-la.

1. **Inicie sessão como administrador de ficheiros ou proprietário no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

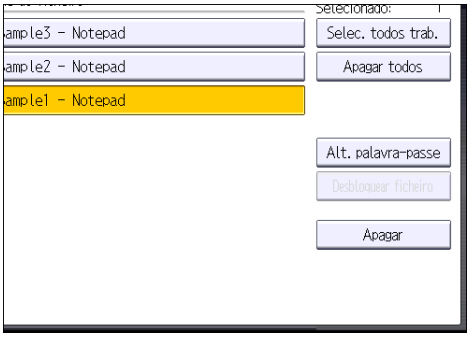
   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].

3. **Prima a tecla [Ecrã inicial] no painel de controlo e prima o ícone [Impressora] no ecrã.**
4. **Prima [Trabalhos de impressão].**

5. **Prima [Trab. impr. bloq.].**



6. **Selecione o ficheiro.**
7. **Prima [Alt. palavra-passe].**



8. **Se aparecer um ecrã para introdução de palavra-passe, introduza a palavra-passe referente ao ficheiro guardado e, em seguida, prima [OK].**

   O ecrã de entrada da palavra-passe não aparecerá se o administrador de ficheiros tiver iniciado sessão.

9. **Introduza a nova palavra-passe para o ficheiro guardado e, em seguida, prima [OK].**
10. **Introduza a palavra-passe de confirmação novamente e, em seguida, prima [OK].**
11. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Desbloquear um ficheiro de impressão bloqueada

Só o administrador de ficheiros pode desbloquear ficheiros.

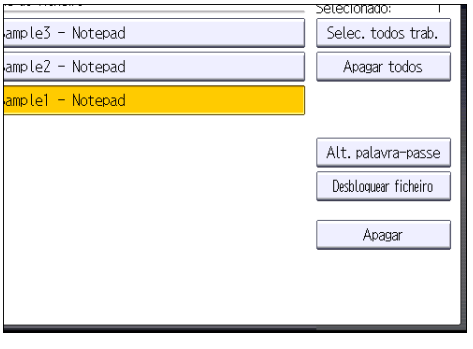
Se especificar [Ligado] para "Melhorar proteção de ficheiros", o ficheiro será bloqueado e ficará inacessível se for introduzida 10 vezes uma palavra-passe inválida. Este capítulo explica como desbloquear ficheiros.

"Melhorar proteção de ficheiros" é uma das funções de segurança avançadas. Para mais informações sobre esta e outras funções de segurança avançadas, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".

1. **Inicie sessão como administrador de ficheiros no painel de controlo.**
2. **Prima a tecla [Ferramentas do utilizador/Contador] para fechar o menu Ferramentas do utilizador.**

   Se aparecer a mensagem "Não possui privilégios para utilizar esta função.", prima [Sair].
3. **Prima a tecla [Ecrã inicial] no painel de controlo e prima o ícone [Impressora] no ecrã.**
4. **Prima [Trabalhos de impressão].**
5. **Prima [Trab. impr. bloq.].**
6. **Selecione o ficheiro.**

   O ícone 🚫 surge ao lado de ficheiros bloqueados pela função Melhorar proteção de ficheiros.
7. **Prima [Desbloquear ficheiro].**



8. **Prima [Sim].**

   O ícone 🚫 desaparece.
9. **Encerre sessão.**

Nota

- Esta também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Imprimir Informações do Utilizador no Papel

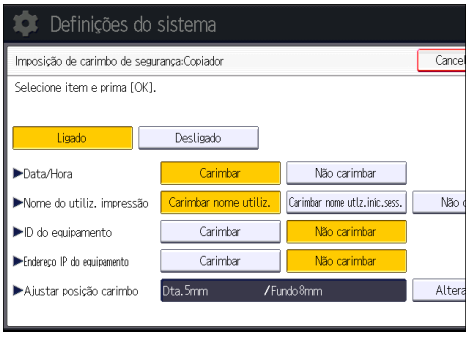
Pode optar por incluir obrigatoriamente nas folhas impressas a hora de início do trabalho de impressão, informações do utilizador que efetua a impressão (nome ou nome de início de sessão), número do equipamento e endereço IP do equipamento. Esta função é chamada Imposição de carimbo de segurança.

A impressão obrigatória das informações do utilizador que efetua a impressão pode desencorajar a fuga de informações. Também pode servir para identificar as fontes de fugas de informação.

A imposição de carimbo de segurança pode ser utilizada com a função de cópia, servidor de documentos e impressão.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Selecione as funções para a imposição de carimbo de segurança.**
   - Para definir a função de cópia para ser carimbada, prima [Imposição carimbo segurança:Copiador].
   - Para definir o Servidor de documentos para ser carimbado, prima [Imposição carimbo segurança:ServDoc].
   - Para definir a função de impressora para ser carimbada, prima [Imposição de carimbo segurança:Impr.].
6. **Prima [Ligado] e, em seguida, selecione os dados a serem carimbados.**

   Para desligar a função de imposição de carimbo de segurança, prima [Desligado].



   - Data/Hora

     A hora de início da impressão será impressa.
   - Nome do utiliz. impressão

     Este será impresso se a autenticação de utilizadores estiver ativada.

- Carimbar nome utiliz.

  O "Nome" em "Nomes" no livro de endereços será impresso.

- Carimbar nome utlz.iníc.sess.

  Será impresso o código de utilizador ou nome de utilizador de início de sessão constante em "Info. Autent." no livro de endereços.

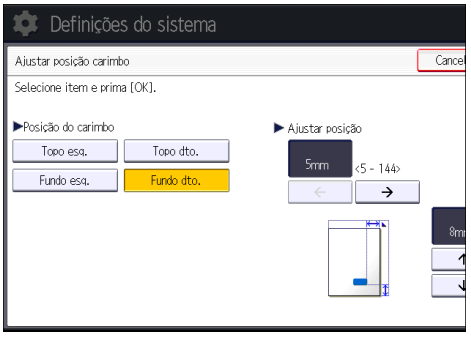
- ID do equipamento

  É impresso o mesmo número apresentado em "Nº de Série do Equipamento" em [Informação].

- Endereço IP do equipamento

  O endereço IP do equipamento será impresso. Se existirem endereços IPv4 e IPv6, será impresso o endereço IPv4. Se não estiverem configurados endereços IP, este campo será deixado em branco.

7. **Prima [Alterar] para "Ajustar posição carimbo".**
8. **Defina a posição do carimbo.**



9. **Prima [OK] duas vezes.**
10. **Encerre sessão.**

7. Gerir o Equipamento

Este capítulo descreve as funções para aumentar a segurança do equipamento e operar o equipamento com eficiência.

Gerir Ficheiros de Registo

Recolher os registos guardados neste equipamento permite-lhe acompanhar dados detalhados referentes ao acesso ao equipamento, à identidade dos utilizadores, à utilização das diversas funções do equipamento e a históricos de erros.

Os registos podem ser eliminados periodicamente para disponibilizar espaço livre no disco rígido.

Os registos podem ser visualizados utilizando o Web Image Monitor ou o servidor de recolha de registos. Os registos recolhidos podem ser convertidos em ficheiros CSV e transferidos todos de uma só vez. Não podem ser lidos diretamente a partir do disco rígido.

Tipos de registo

São guardados 3 tipos de registos neste equipamento: o registo de trabalhos, o registo de acessos e o registo ecológico.

- Registo de trabalhos

  Guarda detalhes de operações relacionadas com ficheiros do utilizador, como cópia, impressão e armazenamento no servidor de documentos, para além de operações do painel de controlo como o envio de ficheiros de digitalização e relatórios de impressão (a lista de configuração, por exemplo).

- Registo de acessos

  Guarda detalhes da atividade de início e encerramento de sessão, operações de ficheiros guardados, como a criação, edição ou eliminação, operações de técnicos de assistência, como a formatação do disco rígido, operações do sistema, como a visualização dos resultados das transferências de registos, e operações de segurança, como especificar definições para encriptação, deteção de acesso sem privilégios, bloqueio de utilizador e autenticação de firmware.

- Registo ecológico

  Guarda detalhes relativos a alimentação elétrica ligada, desligada, transição de estado de alimentação, tempos de execução das tarefas ou intervalo de tempo entre tarefas, consumo de papel por hora, consumo de energia.

Nota

- Para mais informações sobre o servidor de recolha de registos, consulte o manual do utilizador do servidor de recolha de registos.
- Quando utilizar o servidor de recolha de registos, tem de configurar as definições de transferência de registos no servidor de recolha de registos.

Utilizar o Web Image Monitor para Gerir Ficheiros de Registo

Pode especificar os tipos de registo a guardar no equipamento e o nível de recolha de registos. Pode também apagar em conjunto ou transferir ficheiros de registo.

Registos que podem ser geridos utilizando o Web Image Monitor

As tabelas seguintes explicam os itens no registo de trabalhos e registo de acessos que o equipamento cria quando ativa a recolha de registos utilizando o Web Image Monitor. Se necessita de recolher registos, utilize o Web Image Monitor para o configurar. Esta definição pode ser especificada em [Registos] na opção [Configuração] no Web Image Monitor.

Itens das informações de registo de trabalhos

Item de registo de trabalhos	Atributo do tipo de registo	Conteúdos
Copiador: Copiar	Copier: Copying	Detalhes de trabalhos normais e de cópia de teste.
Copiador: Copiar e guardar	Copier: Copying and Storing	Detalhes dos ficheiros guardados no Servidor de documentos que também foram copiados no momento de armazenamento.
Servidor de documentos: Guardar	Document Server: Storing	Detalhes dos ficheiros guardados utilizando o ecrã Servidor de documentos.
Servidor de documentos: Download de ficheiro guardado	Document Server: Stored File Downloading	Detalhes dos ficheiros guardados no Servidor de documentos e transferidos utilizando o Web Image Monitor.
Utilitário: Guardar	Utility: Storing	Detalhes de ficheiros guardados utilizando um utilitário.
Impressão de ficheiro guardado	Stored File Printing	Detalhes dos ficheiros impressos utilizando o ecrã Servidor de documentos.
Scanner: Enviar	Scanner: Sending	Detalhes dos ficheiros de digitalização enviados.

Item de registo de trabalhos	Atributo do tipo de registo	Conteúdos
Scanner: Enviar link de URL e guardar	Scanner: URL Link Sending and Storing	Detalhes dos ficheiros de digitalização guardados no Servidor de documentos. Os respetivos URL foram enviados por e-mail no momento do armazenamento.
Scanner: Enviar e guardar	Scanner: Sending and Storing	Detalhes dos ficheiros de digitalização guardados no servidor de documentos que também foram enviados no momento de armazenamento.
Scanner: Guardar	Scanner: Storing	Detalhes dos ficheiros de digitalização guardados no Servidor de documentos.
Scanner: Download de ficheiro guardado	Scanner: Stored File Downloading	Detalhes dos ficheiros de digitalização guardados no Servidor de documentos e transferidos utilizando o Web Image Monitor ou o Desk Top Editor For Production.
Scanner: Enviar ficheiro guardado	Scanner: Stored File Sending	Detalhes dos ficheiros digitalizados guardados que também foram enviados.
Scanner: Enviar link de URL de ficheiro guardado	Scanner: Stored File URL Link Sending	Detalhes dos ficheiros de digitalização guardados cujos URLs foram enviados por e--mail.
Impressora: A imprimir	Printer: Printing	Detalhes dos trabalhos de impressão normais.
Impressora: Impressão bloqueada (Incompleto)	Printer: Locked Print (Incomplete)	Registo apresentando documentos de Impressão bloqueada temporariamente guardados no equipamento.
Impressora: Impressão bloqueada	Printer: Locked Print	Registo apresentando documentos de Impressão bloqueada temporariamente guardados no equipamento e impressos a partir do painel de controlo ou através do Web Image Monitor.
Impressora: Impressão de teste (Incompleto)	Printer: Sample Print (Incomplete)	Registo apresentando documentos de Impressão de teste temporariamente guardados no equipamento.

Item de registo de trabalhos	Atributo do tipo de registo	Conteúdos
Impressora: Impressão de teste	Printer: Sample Print	Registo apresentando documentos de Impressão de teste temporariamente guardados no equipamento e impressos a partir do painel de controlo ou através do Web Image Monitor.
Impressora: Impressão retida (Incompleto)	Printer: Hold Print (Incomplete)	Registo apresentando documentos de Reter impressão guardados temporariamente no equipamento.
Impressora: Impressão retida	Printer: Hold Print	Registo apresentando documentos de Reter impressão temporariamente guardados no equipamento e impressos a partir do painel de controlo ou através do Web Image Monitor.
Impressora: Impressão guardada	Printer: Stored Print	Detalhes dos ficheiros de Impressão guardada guardados no equipamento.
Impressora: Guardar e impressão normal	Printer: Store and Normal Print	Detalhes dos ficheiros de Impressão guardada impressos no momento de armazenamento (quando "Tipo de trabalho:" estava definido como "Guardar e Imprimir" nas propriedades da impressora).
Impressora: Imprimir ficheiro guardado	Printer: Stored File Printing	Detalhes dos ficheiros de Impressão guardada armazenados a partir do painel de controlo ou do Web Image Monitor.
Impressora: Enviar para o servidor de documentos	Printer: Document Server Sending	Detalhes dos ficheiros guardados no Servidor de documentos quando "Tipo de trabalho:" estava definido como "Servidor de documentos" nas propriedades da impressora.
Imprimir relatórios	Report Printing	Detalhes dos relatórios impressos a partir do painel de controlo.
Imprimir/Enviar por e-mail relatório de resultados	Result Report Printing/ Emailing	Detalhes de resultados de trabalhos impressos a partir do painel de controlo ou notificados por e-mail.
Scanner: Digitalizar com driver TWAIN	Scanner: TWAIN Driver Scanning	Detalhes dos ficheiros de digitalização guardados que foram enviados utilizando o scanner TWAIN de rede.

Item de registo de trabalhos	Atributo do tipo de registo	Conteúdos
Impressora: Impressão de ficheiro de impressão retida	Printer: Hold Print File Printing	Quando um documento é de impressão retida e é guardado temporariamente no equipamento, regista a hora a que um utilizador especifica o documento para ser impresso através do painel de controlo ou do Web Image Monitor.

Itens de informação do registo de acessos

Item de registo de acessos	Atributo do tipo de registo	Conteúdos
Iniciar sessão	Login	A identidade dos utilizadores e a hora em que iniciaram sessão.
Encerrar sessão	Logout	A identidade dos utilizadores e a hora em que encerraram sessão.
Armazenamento de ficheiros	File Storing	Detalhes dos ficheiros guardados no Servidor de documentos.
Eliminação de ficheiro guardado	Stored File Deletion	Detalhes dos ficheiros apagados do Servidor de documentos.
Eliminação de todos os ficheiros guardados	All Stored Files Deletion	Detalhes da eliminação de todos os ficheiros do Servidor de documentos.
Formatação do disco rígido	HDD Format	Detalhes da formatação do disco rígido.
Eliminação de todos os registos	All Logs Deletion	Detalhes da eliminação de todos os registos.
Alteração das definições do registo	Log Setting Change	Detalhes das alterações efetuadas nas definições de registo.
Resultado de transferência de registos	Transfer Log Result	Registo do resultado da transferência de registos para Remote Communication Gate S.

Item de registo de acessos	Atributo do tipo de registo	Conteúdos
Alteração dos itens para recolha de registo	Log Collection Item Change	Detalhes das alterações dos níveis de recolha de registos de trabalho, níveis de recolha de registos de acesso e tipos de registo recolhidos.
Recolher registos de comunicação encriptada	Collect Encrypted Communication Logs	Registo de transmissões encriptadas entre o utilitário, Web Image Monitor ou dispositivos externos.
Violação de acesso	Access Violation	Detalhes das tentativas de acesso falhadas.
Bloqueio	Lockout	Detalhes da ativação da função de bloqueio.
Firmware: Atualização	Firmware: Update	Detalhes das atualizações de firmware.
Firmware: Alteração de estrutura	Firmware: Structure Change	Detalhes das alterações de estrutura que ocorreram quando foi introduzido ou retirado um cartão SD ou quando tiver sido inserido um cartão SD não suportado.
Firmware: Estrutura	Firmware: Structure	Detalhes das verificações de alterações na estrutura de módulo do firmware efetuadas em momentos como quando o equipamento foi ligado.
Alteração da chave de encriptação dos dados do equipamento	Machine Data Encryption Key Change	Detalhes das alterações efetuadas nos códigos de encriptação utilizando a definição de "Alteração da chave de encriptação dos dados do equipamento".
Firmware: Inválido	Firmware: Invalid	Detalhes das verificações de validade do firmware efetuadas em momentos como quando o equipamento foi ligado.
Alteração de data/hora	Date/Time Change	Detalhes das alterações efetuadas nas definições de data e hora.
Alteração do privilégio de acesso ao ficheiro	File Access Privilege Change	Registo para alteração do privilégio de acesso aos ficheiros guardados.

Item de registo de acessos	Atributo do tipo de registo	Conteúdos
Alteração de palavra-passe	Password Change	Detalhes das alterações efetuadas à palavra-passe de início de sessão.
Alteração de administrador	Administrator Change	Detalhes das alterações de administradores.
Alteração do livro de endereços	Address Book Change	Detalhes das alterações efetuadas às entradas do livro de endereços.
Erro de captura	Capture Error	Detalhes dos erros de captura de ficheiros.
Configuração do equipamento	Machine Configuration	Registo de alterações às definições do equipamento.
Backup do livro de endereços	Back Up Address Book	Registo de quando é efetuada uma cópia de segurança dos dados no livro de endereços.
Repor livro de endereços	Restore Address Book	Registo de quando os dados no livro de endereços são restaurados.
Limitação avançada de volumes de utilização para impressão: Resultados de recolha com permissão	Enhanced Print Volume Use Limitation: Tracking Permission Result	Registo de quando ocorre um erro de controlo.
Registo de limpeza de contador: Utilizador(es) selecionado(s)	Counter Clear Result: Selected User(s)	Registo de quando é reposto o contador para um utilizador individual.
Registo de limpeza de contador: Todos os utilizadores	Counter Clear Result: All Users	Registo de quando são repostos os contadores para todos os utilizadores.
Importar informações de definição do equipamento	Import Device Setting Information	Registo de quando é importado um ficheiro de informação de definições de dispositivo.
Exportar informações de definição do equipamento	Export Device Setting Information	Registo de quando é exportado o ficheiro de informação de definições de dispositivo.

Item de registo de acessos	Atributo do tipo de registo	Conteúdos
Ao criar/apagar pastas	Creating/Deleting Folders	Registo que informa quando são criadas e eliminadas pastas.
Edição de ficheiro guardado	Stored File Editing	Registo de edição de um ficheiro.
Inserção noutro ficheiro	Insertion into another File	Registo de inserção de um ficheiro noutro ficheiro.

Não existe nenhum registo de "Iniciar sessão" feito para SNMPv3.

Se o disco rígido for formatado, todas as entradas de registo até ao momento da formatação serão apagadas e é criada uma entrada de registo indicando a conclusão da formatação.

"Violação de acesso" indica que o sistema tem sido, com frequência, alvo de ataques remotos de DoS envolvendo tentativas de início de sessão através da autenticação de utilizador.

O primeiro registo criado após a ligação da alimentação é o registo "Firmware: Estrutura".

Itens de informação do registo ecológico

Item do registo ecológico	Atributo do tipo de registo	Conteúdos
Equipamento ligado	Main Power On	Registo de quando o interruptor de alimentação principal é ligado.
Equipamento desligado	Main Power Off	Registo de quando o interruptor de alimentação principal é desligado.
Registo de transição para o estado ligado/desligado	Power Status Transition Result	Registo dos resultados de transição para o estado ligado/desligado.
Informações relacionadas com trabalho	Job Related Information	Registo de informações relacionadas com trabalhos.
Consumo de papel	Paper Usage	Registo da quantidade de papel utilizada.
Consumo de energia	Power Consumption	Registo do consumo de energia.

Atributos dos registos que é possível transferir

Se utilizar o Web Image Monitor para transferir registos, é criado um ficheiro CSV com os itens de informação apresentados na tabela seguinte.

Note que um campo em branco indica um item não incluído num registo.

Formato de saída do ficheiro

- Conjunto do código de carateres: UTF-8
- Formato de saída: CSV (Comma-Separated Values)
- Nomes de ficheiro de registos de trabalhos e de registos de acessos: "machine name +_log.csv"
- Nomes de ficheiro para registos ecológicos: "machine name+_ecolog.csv"

Ordem das entradas de registo

As entradas de registo são impressas por ordem crescente de acordo com a ID de registo.

Estrutura do ficheiro

O título dos dados é impresso na primeira linha (linha de cabeçalho) do ficheiro.

Diferenças na formatação de dados de registo

- Registo de trabalhos

  Surgem várias linhas por ordem de itens comuns (registo de trabalhos e registo de acessos), Origem (dados de entrada dos trabalhos) e Destino (dados de saída dos trabalhos). A ID de registo atribuída é a mesma para todas as linhas correspondentes a uma entrada de registo de trabalho única.

	Start Date/Time	···	Result	···	Access Result	Source	···	Print File Name	Target	···	Stored File Name
1	20XX-12-03T15:43:03,0	···	Completed	···			···			···	
2		···	Completed	···		Report	···			···	
3		···	Completed	···			···		Print	···	

CJD022

1. **Itens comuns**

   Cada item da lista de itens comuns é apresentado numa linha diferente.

2. **Source**

   "Result" e "Status" surgem nos itens comuns e nos dados de entrada do registo do trabalho.

   Se houver várias origens, surgem várias linhas.

3. **Target**

   "Result" e "Status" surgem nos itens comuns e nos dados de saída do registo do trabalho.

   Se houver vários destinos, surgem várias linhas.

- Registo de acesso

  Os itens comuns e as entradas do registo de acessos surgem em linhas diferentes.

- Registo ecológico

As entradas do registo ecológico surgem em linhas diferentes.

Itens comuns (registo de trabalhos e registo de acessos)

Start Date/Time

Indica a data e hora de início de uma operação ou ocorrência.

End Date/Time

Indica a data e hora de fim de uma operação ou ocorrência.

Log Type

Detalhes do tipo de registo.

Para mais informações sobre os itens de informação contidos em cada tipo de registo, consulte Pág. 178 "Registos que podem ser geridos utilizando o Web Image Monitor".

Result

Indica o resultado de uma operação ou ocorrência.

Os itens de registo seguintes apenas são gravados quando as operações registadas são executadas com êxito:

"Document Server: Stored File Downloading", "Stored File Printing", "Scanner: Storing", "Scanner: Stored File Sending" e "Printer: Stored File Printing" (registos de trabalhos) e "File Storing" e "Stored File Deletion" (registos de acessos).

Valor	Conteúdos
Succeeded	A operação ou ocorrência foi concluída com êxito.
Failed	A operação ou ocorrência não teve êxito.
<Em branco>	A operação ou ocorrência ainda está em curso.

Operation Method

Indica o procedimento da operação.

Valor	Conteúdos
Control Panel	Painel de controlo
Driver	Driver
Utility	Utilitário
Web	Web
Email	E-mail

Status

Indica o estado de uma operação ou ocorrência.

Valor	Conteúdos
Completed	A operação ou ocorrência foi concluída com êxito na entrada de um registo de trabalho.
Failed	A operação ou ocorrência não teve êxito na entrada de um registo de trabalho.
Succeeded	A operação ou ocorrência foi concluída com êxito na entrada de um registo de acesso.
Password Mismatch	Ocorreu um erro de acesso em virtude de as palavras-passes não coincidirem.
User Not Programmed	Ocorreu um erro de acesso porque o utilizador não está registado.
Other Failures	Ocorreu um erro de acesso devido a uma falha não especificada.
User Locked Out	Ocorreu um erro de acesso porque o utilizador está bloqueado.
File Limit Exceeded	Ocorreu um erro de acesso porque o limite de ficheiros foi ultrapassado.
Transfer Cancelled	Ocorreu um erro de acesso devido a um cancelamento de transferência.
Power Failure	Ocorreu um erro de acesso devido a uma falha de energia.
Lost File	Ocorreu um erro de acesso porque o ficheiro foi perdido.
Functional Problem	Ocorreu um erro de acesso devido a um problema funcional.
Communication Failure	Ocorreu um erro de acesso devido a uma falha de comunicação.
Communication Result Unknown	Ocorreu um erro de acesso devido a um resultado de comunicação desconhecido.
Failure in some or all parts	A limpeza do contador específico do utilizador ou do contador de todos os utilizadores falhou.

Valor	Conteúdos
Importing/Exporting by Other User	A importação ou exportação está a ser executada por outro utilizador.
Connection Failed with Remote Machine	A ligação a um destino de saída falhou.
Write Error to Remote Machine	Ocorreu um erro ao escrever para um destino de saída.
Specified File: Incompatible	O ficheiro especificado é incompatível.
Specified File: Format Error	Ocorreu um erro de formato com o ficheiro especificado.
Specified File: Not Exist	Não é possível localizar o ficheiro especificado.
Specified File: No Privileges	Falta o privilégio para aceder ao ficheiro especificado.
Specified File: Access Error	Ocorre um erro ao aceder ao ficheiro especificado.
Memory Storage Device Full	O suporte de dados externo está cheio.
Memory Storage Device Error	Foi encontrada uma anomalia no suporte de dados externo.
Encryption Failed	A encriptação falhou.
Decoding Failed	A descodificação falhou.
Common Key Not Exist	Falta a chave comum.
Connection Error	Ocorreu um erro de comunicação.
Specified Server Error	Ocorreu um erro de acesso porque o servidor não está configurado corretamente.
Specified Client Error	Ocorreu um erro de acesso porque o cliente não está configurado corretamente.
Authentication Settings Mismatch	As especificações do livro de endereços não correspondem.
Authentication Method Mismatch	Os métodos de autenticação não correspondem.
Maximum Limit of Registered Number	O número máximo de equipamentos que podem ser registados.
Invalid Password	A palavra-passe introduzida não é válida.

Valor	Conteúdos
Processing	O trabalho está a ser processado.
Error	Ocorreu um erro.
Suspended	O trabalho foi suspenso.

Cancelled: Details

Indica o estado no qual a operação ou ocorrência não teve êxito.

Valor	Conteúdos
Cancelled by User	Um utilizador cancelou a operação.
Input Failure	Uma entrada foi terminada de forma anormal.
Output Failure	Uma saída foi terminada de forma anormal.
Other Error	Foi detetado um erro antes da execução de um trabalho ou ocorreram outros erros.
Power Failure	Falha de energia.
External Charge Unit Disconnected	O dispositivo de gestão foi desligado durante o funcionamento.
Insufficient No. of Original for Overlay	Faltavam páginas de um manuscrito durante a execução da cópia sobreposta.
Exceed Max. Stored Page (File Storage)	A capacidade de armazenamento de páginas no servidor de documentos atingiu o limite.
Exceed Max. Stored File (File Storage)	A capacidade de armazenamento de documentos no servidor de documentos atingiu o limite.
Hard Disk Full (File Storage Memory)	A capacidade do disco rígido no servidor de documentos atingiu o limite.
Exceeded Max. Email Size	Foi atingido o limite do tamanho do e-mail.
Exceeded Max. File Size	O limite de tamanho de um documento foi atingido.
Scanner Error	Ocorreu um erro com o alimentador automático de documentos.
Timeout	Foi atingido o tempo limite.

Valor	Conteúdos
Exceed Max. Stored Page (Image Area)	O número de páginas que podem ser capturadas atingiu o limite.
Hard Disk Full (Image Area)	A capacidade do disco rígido para captura atingiu o limite.
Specified Folder to Store does not Exist	Não é possível localizar a pasta de armazenamento do ficheiro especificada.
Password for Folder Specified to Store is Incorrect	A palavra-passe da pasta de armazenamento do ficheiro especificada está incorreta.
Folder is Locked	A pasta está bloqueada.
Memory Full	O intervalo de memória para o processamento de dados está cheio.
Print Data Error	Foi efetuada uma tentativa para utilizar uma PDL ou uma porta não instalada no equipamento.
Data Transfer Interrupted	Os seguintes casos são registados: • O driver utilizado não coincide. • Ocorre uma anomalia de rede.
Over Job Limit	O número de trabalhos que é possível receber atingiu o limite.
Specifying Destination Error	Foi especificado um endereço ilegal ou um endereço com 41 ou mais dígitos.
Authentication Failed (Access Restricted)	A autenticação do dispositivo falhou.
No Privilege	O utilizador não tem permissão para aceder a um documento ou função.
Unavailable Size to Store	O tamanho de papel especificado (incluindo tamanhos personalizados) não pode ser guardado.
Transmission Failed (Data Deleted)	Um documento foi eliminado ou um documento não entregue excedeu o respetivo tempo de espera e foi eliminado.
Not Entered Document Password	A palavra-passe de um documento não foi introduzida.
Connection Failed with Destination	Não foi localizado o servidor ou a pasta especificado(a).

Valor	Conteúdos
Authentication Failed with Destination	A autenticação no destino falhou.
Transmission Failed with Memory Full	A memória do destino está cheia.
Invalid Device Certificate	Os seguintes casos são registados: • O certificado do dispositivo está em falta. • O período de validade expirou. • Se os endereços de e-mail do administrador e do certificado não coincidem.
Invalid Expiration Date: Destination's Certificate	O período de validade do certificado do destino expirou.
Invalid Device/Destination's Certificate	O certificado do destino e o certificado do dispositivo são ambos inválidos.
Print Cancelled (Error)	O trabalho de impressão foi cancelado devido a um erro de sistema.

User Entry ID

Indica a ID de entrada do utilizador.

Esta é uma ID hexadecimal que identifica utilizadores que executaram operações relacionadas com registo de trabalhos ou com registo de acessos.

Valor	Conteúdos
0x00000000	Operações do sistema, operações que foram realizadas por utilizadores não autenticados
0x00000001 - 0xffffeff	Para utilizadores gerais e códigos de utilizador
0xffffff80	Operações do sistema
0xffffff81	Operações do sistema, operações que foram realizadas por utilizadores não autenticados
0xffffff86	Supervisor
0xffffff87	Administrador
0xffffff88	Administrador 1

Valor	Conteúdos
0xffffff89	Administrador 2
0xffffff8a	Administrador 3
0xffffff8b	Administrador 4

User Code/User Name

Identifica o código ou o nome do utilizador do utilizador que realizou a operação.

Se um administrador efetuou a operação, esta ID contém o nome utilizador de início de sessão do administrador.

Log ID

Identifica a ID atribuída ao registo.

Esta é uma ID hexadecimal que identifica o registo.

Itens de informação do registo de acessos

Access Log Type

Indica o tipo de acesso.

Valor	Conteúdos
Authentication	Acesso de autenticação do utilizador
Stored File	Acesso a ficheiros guardados
System	Acesso ao sistema
Network Attack Detection/ Encrypted Communication	Acesso a ataque da rede ou comunicação encriptada
Firmware	Acesso de verificação do firmware
Address Book	Acesso ao livro de endereços
Device Settings	Alterações efetuadas numa definição no menu Ferramentas do utilizador.

Authentication Server Name

Indica o nome do servidor onde foi tentada a autenticação pela última vez.

No. of Authentication Server Switches

Indica o número vezes que ocorreu a mudança de servidores quando o servidor de autenticação não estava disponível.

Pode verificar se o servidor de autenticação está disponível ou não.

O número de alteração de servidores indicado é de 0 a 4.

"0" indica que o servidor de autenticação está disponível.

Logout Mode

Modo de encerrar sessão.

Valor	Conteúdos
by User's Operation	Encerramento manual da sessão pelo utilizador
by Auto Logout Timer	Encerramento automático da sessão ao fim de um tempo limite

Login Method

Indica a rota através da qual é recebido o pedido de autenticação.

Valor	Conteúdos
Control Panel	O início de sessão foi realizado utilizando o painel de controlo.
via Network	O início de sessão foi realizado remotamente utilizando um computador da rede.
Others	O início de sessão foi realizado utilizando outro método.

Login User Type

Indica o tipo de utilizador de início de sessão.

Valor	Conteúdos
User	Utilizador geral
Guest	Utilizador visitante
User Administrator	Administrador de utilizadores
Machine Administrator	Administrador do equipamento
Network Administrator	Administrador de rede
File Administrator	Administrador de ficheiros

Valor	Conteúdos
Supervisor	Supervisor
Customer Engineer (Service Mode)	Técnico de assistência
Others	Pedidos de início de sessão de outros utilizadores além dos especificados acima

Target User Entry ID

Indica a ID do utilizador visado.

Esta é uma ID hexadecimal que indica utilizadores aos quais as definições seguintes se aplicam:

- Lockout
- Password Change

Target User Code/User Name

Código ou nome de utilizador cujos dados foram acedidos.

Se tiverem sido acedidos os dados do administrador, é registado o nome de utilizador do administrador.

Address Book Registration No.

Indica o número de registo do utilizador que realiza a operação.

Address Book Operation Mode

Indica o método aplicado para alterar os dados registados no livro de endereços.

Address Book Change Item

Indica o item que foi alterado no livro de endereços.

Address Book Change Request IP Address

Indica o tipo de endereço IP (IPv4/IPv6) do utilizador do livro de endereços.

Lockout/Release

Indica o estado do bloqueio.

Valor	Conteúdos
Lockout	Ativação do bloqueio por palavra-passe
Release	Desativação do bloqueio por palavra-passe

Lockout/Release Method

Indica o método aplicado para cancelar o bloqueio.

Valor	Conteúdos
Manual	O equipamento é desbloqueado manualmente.
Auto	O equipamento é desbloqueado pelo temporizador de bloqueio da conta.

Lockout Release Target Administrator

Indica que administradores são desbloqueados ao cancelar o bloqueio.

Counter to Clear

Indica qual é o contador reiniciado para cada utilizador.

Export Target

Indica as definições para incluir no ficheiro de definições do dispositivo a exportar.

Valor	Conteúdos
System Settings	Definições do Sistema
Copier Features	Funções de copiador
Printer Features	Funções de Impressora
Scanner Features	Funções de Scanner
Program (Copier)	Programar (copiador)
Program (Scanner)	Programar (scanner)
Program (Document Server)	Programar (Servidor de documentos)
Browser Features	Funções de Browser
Web Image Monitor Setting	Definição do Web Image Monitor
Web Service Settings	Definições do serviço Web
System/Copier SP	SP de sistema/copiador
Scanner SP	SP de scanner
Printer SP	SP de impressora

Target File Name

Indica o nome do ficheiro de informações do dispositivo a importar ou exportar.

Stored File ID

Identifica um ficheiro criado ou eliminado.

Esta é uma ID hexadecimal que indica ficheiros guardados que foram criados ou eliminados.

Stored File Name

Indica o nome de um ficheiro criado ou eliminado.

Delete File Type

Indica o tipo de eliminação do ficheiro.

Valor	Conteúdos
Delete Normal File	Eliminação normal do ficheiro
Delete Editing File	Eliminação durante a edição
Auto Delete	Eliminação automática do ficheiro
Others	Eliminação do ficheiro por outra razão

Folder Number

Indica o número da pasta.

Folder Name

Indica o nome da pasta.

Creating/Deleting Folders

Indica as operações realizadas nas pastas.

Valor	Conteúdos
Delete Folder	Pasta eliminada
New Folder	Pasta criada

File Location

Indica a origem de todos os ficheiros eliminados. Document Server" indica a eliminação de todos os ficheiros do disco rígido do equipamento.

Collect Job Logs

Indica o estado da definição de recolha de registos de trabalhos.

Valor	Conteúdos
Active	A definição de recolha de registos de trabalhos está ativada.

Valor	Conteúdos
Inactive	A definição de recolha de registos de trabalhos está desativada.
Not Changed	Não foram efetuadas alteradas na definição de recolha de registos de trabalhos.

Collect Access Logs

Indica o estado da definição de recolha de registos de acessos.

Valor	Conteúdos
Active	A definição de recolha de registos de acessos está ativada.
Inactive	A definição de recolha de registos de acessos está desativada.
Not Changed	Não foram efetuadas alterações na definição de recolha de registos de acessos.

Collect Eco-friendly Logs

Indica o estado da definição de recolha de registos ecológicos.

Valor	Conteúdos
Active	A definição de recolha de registos ecológicos está ativada.
Inactive	A definição de recolha de registos ecológicos está desativada.
Not Changed	Não foram efetuadas alterações na definição de recolha de registos ecológicos.

Transfer Logs

Indica o estado da definição de transferência de registos.

Valor	Conteúdos
Active	A definição de transferência de registos está ativada.
Inactive	A definição de transferência de registos está desativada.
Not Changed	Não foram efetuadas alterações na definição de transferência de registos.

Log Type

Se a definição do nível de recolha de um registo foi alterada, esta função indica os detalhes da alteração.

Valor	Conteúdos
Job Log	Registo de trabalhos
Access Log	Registo de acesso
Eco-friendly Log	Registo ecológico

Log Collect Level

Indica o nível de recolha de registos.

Valor	Conteúdos
Level 1	Nível 1
Level 2	Nível 2
User Settings	Definições do utilizador

Encryption/Cleartext

Indica se a encriptação de comunicação está ativada ou desativada.

Valor	Conteúdos
Encryption Communication	A encriptação está ativada.
Cleartext Communication	A encriptação está desativada.

Machine Port No.

Indica o número da porta do equipamento.

Protocol

Protocolo de destino.

"Unknown" indica que o protocolo do destino não foi identificado.

IP Address

Endereço IP de destino.

Port No.

Número de porta de destino.

Os números de porta são indicados em números decimais.

MAC Address

Endereço MAC (físico) de destino.

Primary Communication Protocol

Indica o protocolo de comunicação primário.

Secondary Communication Protocol

Indica o protocolo de comunicação secundário.

Encryption Protocol

Indica o protocolo utilizado para encriptar a comunicação.

Communication Direction

Indica a direção de comunicação.

Valor	Conteúdos
Communication Start Request Receiver (In)	O equipamento recebeu um pedido para iniciar a comunicação.
Communication Start Request Sender (Out)	O equipamento enviou um pedido para iniciar a comunicação.

Communication Start Log ID

Indica a ID de registo para a hora de início da comunicação.

Esta é uma ID hexadecimal que indica a hora a que a comunicação teve início.

Communication Start/End

Indica as horas a que a comunicação teve início e terminou.

Network Attack Status

Indica o estado do equipamento quando ocorrem os ataques à rede.

Valor	Conteúdos
Violation Detected	Foi detetado um ataque à rede.
Recovered from Violation	A rede recuperou de um ataque.
Max. Host Capacity Reached	O equipamento ficou inoperacional em virtude de o volume de dados recebidos ter atingido a capacidade máxima do host.
Recovered from Max. Host Capacity	O equipamento ficou novamente operacional após a redução do volume de dados recebidos.

Network Attack Type

Identifica tipos de ataques à rede.

Valor	Conteúdos
Password Entry Violation	Descodificação da palavra-passe
Device Access Violation	Ataque de negação de serviço (DoS)
Request Falsification Violation	Falsificação de pedido

Network Attack Type Details

Indica os detalhes dos tipos de ataque à rede.

Valor	Conteúdos
Authentication Error	Erro de autenticação
Encryption Error	Erro de encriptação

Network Attack Route

Identifica a rota do ataque à rede.

Valor	Conteúdos
Attack from Control Panel	Ataque através de uma operação não autorizada utilizando o painel de controlo do equipamento
Attack from Other than Control Panel	Ataque por outros meios que não através de uma operação não autorizada utilizando o painel de controlo do equipamento

Login User Name used for Network Attack

Identifica o nome de utilizador de início de sessão com o qual foi efetuado o ataque à rede.

Add/Update/Delete Firmware

Indica o método utilizado para adicionar, atualizar ou eliminar o firmware do equipamento.

Valor	Conteúdos
Updated with SD Card	Foi utilizado um SD card para realizar a atualização do firmware.
Added with SD Card	Foi utilizado um SD card para instalar o firmware.

Valor	Conteúdos
Deleted with SD Card	Foi utilizado um SD card para eliminar o firmware.
Moved to Another SD Card	O firmware foi movido para outro SD card.
Updated via Remote	O firmware foi atualizado a partir de um computador remoto.
Updated for Other Reasons	A atualização do firmware foi realizada utilizando outro método além dos indicados acima.

Module Name

Nome do módulo de firmware.

Parts Number

Número da parte do módulo de firmware.

Version

Versão do firmware.

Machine Data Encryption Key Operation

Indica o tipo de operação da chave de encriptação executado.

Valor	Conteúdos
Back Up Machine Data Encryption Key	Foi criada a cópia de segurança de uma chave de encriptação.
Restore Machine Data Encryption Key	Foi reposta uma chave de encriptação.
Clear NVRAM	A NVRAM foi limpa.
Start Updating Machine Data Encryption Key	Foi iniciada a atualização da chave de encriptação.
Finish Updating Machine Data Encryption Key	Foi concluída a atualização de um código de encriptação.

Machine Data Encryption Key Type

Identifica o tipo de chave de encriptação.

Valor	Conteúdos
Encryption Key for Hard Disk	Chave de encriptação para disco rígido

Valor	Conteúdos
Encryption Key for NVRAM	Chave de encriptação para NVRAM
Device Certificate	Certificação do dispositivo

Validity Error File Name

Indica o nome do ficheiro onde foi detetado um erro de validade.

Configuration Category

Indica as categorias com definições alteradas.

Valor	Conteúdos
User Lockout Policy	Política de bloqueio do utilizador
Auto Logout Timer	Temporizador de encerramento automático de sessão
Device Certificate	Certificação do dispositivo
IPsec	IPsec
Compulsory Security Stamp	Carimbo de segurança obrigatório
S/MIME	S/MIME
WIM Auto Logout Timer	Temporizador de encerramento automático de sessão do Web Image Monitor
Extended Security	Segurança Avançada
Firmware Update Start	Atualização do firmware
Prohibit printing stored files from Web Image Monitor	Prohibit printing stored files from Web Image Monitor

Configuration Name / Configuration Value

Indica os atributos das categorias.

Indica os valores dos atributos.

Atributo	Descrição
Lockout	Se o bloqueio está ativo (Active) ou inativo (Inactive) fica gravado.

Atributo	Descrição
Number of Attempts before Lockout	O número de vezes que um utilizador pode introduzir uma palavra-passe de início de sessão fica gravado.
Lockout Release Timer	Se o temporizador de libertação de bloqueio está ativo (Active) ou inativo (Inactive) fica gravado.
Lock Out User for	O tempo até à libertação do bloqueio fica gravado.
Auto Logout Timer	É registado se o temporizador de encerramento automático de sessão está definido para (On) ou (Off).
Auto Logout Timer(seconds)	O tempo até à operação do encerramento automático de sessão fica gravado.
Operation Mode	O tipo de operação fica gravado.
Certificate No.	O número do certificado a ser utilizado fica gravado.
Certificate No. : IEEE 802. 1X (WPA/WPA2)	O número do certificado para aplicações fica gravado. Quando não é utilizado nenhum certificado, fica gravado "Do not Use".
Certificate No. : S/MIME	O número do certificado para aplicações fica gravado. Quando um certificado não é utilizado, fica gravado "Do not Use".
Certificate No. : IPsec	O número do certificado para aplicações fica gravado. Quando não é utilizado nenhum certificado, fica gravado "Do not Use".
Certificate No. : Digital Signature PDF	O número do certificado para aplicações fica gravado. Quando não é utilizado nenhum certificado, fica gravado "Do not Use".
Certificate No. : Digital Signature PDF/A	O número do certificado para aplicações fica gravado. Quando não é utilizado nenhum certificado, fica gravado "Do not Use".
IPsec	Se IPsec está ativo (Active) ou inativo (Inactive) fica gravado.
Encryption Key Auto Exchange: Setting1-4: Remote Address	O endereço remoto fica gravado.

Atributo	Descrição
Encryption Key Auto Exchange: Setting1-4, Default: Security Level	O nível de segurança fica gravado. Quando [Autenticação apenas] é selecionado, fica gravado "Authentication Only". Quando [Autenticação e baixa encriptação] é selecionado, fica gravado "Authentication and Low Level Encryption". Quando [Autenticação e elevada encriptação] é selecionado, fica gravado "Authentication and High Level Encryption". Quando [Definições do utilizador] é selecionado, fica gravado "User Settings".
Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	O método de autenticação utilizado para o formato da troca de chave automática fica gravado. Fica gravado "PSK" ou "Certificate".
Compulsory Security Stamp	Fica gravado se [Imposição de carimbo de segurança] é definido como (On) ou (Off).
Scanner: Email Sending	A assinatura fica gravada quando o scanner é utilizado para enviar e-mail.
Document Server (Utility): Stored File Transferring	A assinatura fica gravada quando o Servidor de documentos (Utilitário) é utilizado para transmitir os documentos nele guardados.
WIM Auto Logout Timer (minutes)	O registo do temporizador automático para encerrar a sessão no Web Image Monitor é registado em variações de um minuto.
Update Firmware	É gravada uma entrada de registo que regista alterações na definição [Atualização do firmware]. É gravado "Prohibit" ou "Do not Prohibit".
Change Firmware Structure	É gravada uma entrada de registo que regista alterações na definição [Alterar estrutura do firmware]. É gravado "Prohibit" ou "Do not Prohibit".
Firmware Update Start	É gravada uma entrada de registo que regista uma atualização de firmware.

Atributo	Descrição
Prohibit printing stored files from Web Image Monitor	É gravada uma entrada de registo que regista alterações na definição [Prohibit printing stored files from Web Image Monitor]. É gravado "Prohibit" ou "Do not Prohibit".

Destination Server Name

Indica o nome do servidor de destino para o qual a informação de controlo não foi enviada se o tipo de registo for "Enhanced Print Volume Use Limitation: Tracking Permission Result".

Indica o nome do servidor a partir do qual é enviado o pedido de exportação ou importação de dados se o tipo de registo for para a importação ou exportação das informações de preferências.

HDD Format Partition

Indica o motivo para formatar o disco rígido.

Valor	Conteúdos
HDD Exchange	O disco rígido foi substituído.
Problem with HDD Encryption Key	Existe um problema com a chave de encriptação do disco rígido.
Problem with Disk Label	Não é possível ler a etiqueta do disco.
Problem with File System	Há um problema com o sistema de ficheiros.

Access Result

Indica os resultados de operações registadas.

Valor	Conteúdos
Completed	Uma operação concluída com êxito.
Failed	Uma operação não concluída com êxito.

Registo de trabalhos (origem)

Source

Indica a origem do ficheiro do trabalho.

Valor	Conteúdos
Scan File	O ficheiro do trabalho foi digitalizado.
Stored File	O ficheiro do trabalho foi guardado no disco rígido.
Printer	O ficheiro do trabalho foi enviado a partir do driver de impressão.
Report	O ficheiro do trabalho era um relatório impresso.

Start Date/Time

Indica o início das operações "Scan File", "Received File" e "Printer".

End Date/Time

Indica o fim das operações "Scan File", "Received File" e "Printer".

Stored File ID

Indica a ID dos dados produzidos como ficheiro guardado.

Esta é uma ID decimal que identifica o ficheiro guardado.

Stored File Name

Nomes de ficheiros "Stored File".

Folder Number

Indica o número da pasta na qual o ficheiro foi guardado.

Folder Name

Indica o nome da pasta na qual o ficheiro foi guardado.

Print File Name

Nome de ficheiros "Printer".

Registo de trabalhos (destino)

Target

Tipo de destino do trabalho.

Valor	Conteúdos
Print	Print
Store	Guardar
Send	Enviar

Start Date/Time

Indica o início das operações "Print", "Store" e "Send".

End Date/Time

Indica o fim das operações "Print", "Store" e "Send".

Destination Name

Nomes de destinos "Send".

Destination Address

Endereço IP, caminho ou endereço de e-mail dos destinos "Send".

Stored File ID

Indica a ID dos dados produzidos como um ficheiro guardado.

Esta é uma ID decimal que identifica o ficheiro guardado.

Stored File Name

Indica o nome do ficheiro guardado quando o tipo de destino é "Store".

Folder Number

Indica o número da pasta onde guardou o ficheiro.

Folder Name

Indica o nome da pasta onde guardou o ficheiro.

Itens de informação do registo ecológico

Start Date/Time

A data e hora de início do evento fica gravada.

End Date/Time

A data e hora do final do evento fica gravada.

Log Type

O tipo de registo ecológico fica gravado.

Valor	Conteúdos
Main Power On	Alimentação ligada
Main Power Off	Alimentação desligada
Power Status Transition Result	Resultado da transição do estado da alimentação
Job Related Information	Informações relacionadas com o trabalho
Paper Usage	Utilização de papel

Valor	Conteúdos
Power Consumption	Consumo de energia

Log Result

É apresentado se o evento terminou ou não.

Valor	Conteúdos
Completed	Concluído
Failed	Falhou

Result

O resultado do evento é gravado.

Valor	Conteúdos
Succeeded	Com êxito
Failed	Falhou

Log ID

Identifica a ID atribuída ao registo. Esta é uma ID hexadecimal que identifica o registo.

Power Mode

O estado de alimentação elétrica do equipamento (após transição de estado) fica gravado.

Valor	Conteúdos
Standby	Estado de modo de espera
Low Power	Estado de baixo consumo
Silent	Estado silencioso
HDD On	Estado ligado do disco rígido
Engine Off	Estado desligado do motor
Controller Off	Estado desligado da controladora
STR	Estado STR
Silent Print	Estado de impressão silenciosa

Valor	Conteúdos
Low Power Print	Estado de impressão de baixo consumo
Fusing Unit Off	Estado desligado da unidade de fusão

Log Type

O tipo de registo de trabalho fica gravado.

Job Interval (seconds)

Indica o tempo decorrido desde o início do trabalho anterior até ao início do trabalho atual.

Job Duration (seconds)

Indica o tempo decorrido desde o início de um trabalho até à respetiva conclusão.

Paper Usage (Large Size)

Indica o número de impressões de um lado por hora em papel de formato grande.

Formato grande significa A3 (11 × 17 polegadas) ou maior.

Paper Usage (Small Size)

Indica o número de impressões de um lado por hora em papel de formato pequeno.

Formato pequeno significa menor que A3 (11 × 17 polegadas).

Detected Power

O estado do consumo de energia do equipamento é medido e registado no registo enquanto o equipamento é utilizado.

Valor	Conteúdos
Controller Standby	Modo de espera da controladora
STR	Modo STR (Suspend to RAM)
Main Power Off	O interruptor de alimentação principal está desligado.
Scanning/Printing	Digitalização e impressão simultâneas
Printing	Estado de impressão do equipamento
Scanning	Estado de digitalização do equipamento
Engine Standby	Estado de modo de espera do motor
Engine Low	Estado de baixo consumo do motor
Engine Night	Estado silencioso do motor

Valor	Conteúdos
Engine Total	Consumo de eletricidade total do equipamento
Fusing Unit Off	Estado desligado da unidade de fusão

Power Consumption(Wh)

Indica o consumo de energia em cada estado de alimentação.

Especificar as definições da recolha de registos

Ative as definições de recolha para cada tipo de registo e configure o nível de recolha.

Nível de recolha do registo de trabalhos

Se "Nível de recolha do registo de trabalhos" estiver definido como [Nível 1], todos os registos de trabalhos são recolhidos.

Nível de recolha do registo de acessos

Se "Nível de recolha do registo de acessos" estiver definido como [Nível 1], os seguintes itens são gravados no registo de acesso:

- Formatação do disco rígido
- Eliminação de todos os registos
- Alteração das definições do registo
- Alteração dos itens para recolha de registo

Se "Nível de recolha do registo de acessos" estiver definido como [Nível 2], todos os registos de acesso são recolhidos.

Nível de recolha dos registos ecológicos

Se "Nível de recolha dos registos ecológicos" estiver definido como [Nível 1], os registos ecológicos não são recolhidos.

Se "Nível de recolha dos registos ecológicos" estiver definido como [Nível 2], todos os registos ecológicos são recolhidos.

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Registos] sob "Definições do dispositivo".**
4. **Selecione [Ativo] para cada função: "Recolher registos de trabalhos", "Recolher registos de acesso" e "Recolher registos ecológicos".**

5. **Especifique o nível de de recolha para cada função, "Nível de recolha do registo de trabalhos", "Nível de recolha do registo de acessos" e "Nível de recolha dos registos ecológicos".**

   Quando um nível é alterado, o estado da seleção dos detalhes do registo altera-se de acordo com o nível.

   Para alterar itens individuais dos detalhes do registo, configure a definição para cada item. Mesmo que o nível de recolha esteja definido para [Nível 1] ou [Nível 2], quando cada item dos detalhes de registo for alterado, o nível muda para [Definições do utilizador].

6. **Clique em [OK].**
7. **É apresentada a mensagem "A atualizar...". Aguarde cerca de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se o ecrã anterior não aparecer novamente depois de clicar em [OK], aguarde uns segundos e clique no botão [Atualizar] do web browser.

8. **Encerre sessão.**

Nota

- Quanto maior for o valor da definição de "Nível de recolha do registo de acessos", mais registos são recolhidos.

Transferir registos

Utilize o seguinte procedimento para converter os registos guardados no equipamento num ficheiro CSV para transferência em lote simultânea.

Para recolher registos, configure como [Ativo] a definição de recolha para o registo de trabalhos, o registo de acessos e o registo ecológico.

Esta definição pode ser especificada em [Registos] na opção [Configuração] no Web Image Monitor.

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Download de registos] sob "Definições do dispositivo".**
4. **Selecione o tipo de registo para transferir a partir da caixa "Registos para download".**

   O registo de segurança inclui 2 tipos de registos: registos de trabalhos e registos de acesso.

5. **Clique em [Download].**
6. **Especifique a pasta na qual pretende guardar o ficheiro.**
7. **Clique em [Retroceder].**
8. **Encerre sessão.**

Nota

- Os registos transferidos contêm dados gravados até ao momento em que tiver clicado no botão [Download]. Quaisquer registos gravados após o botão [Download] ser clicado não serão transferidos. O campo "Result" da entrada no registo para trabalhos não concluídos ficará em branco.
- O tempo de transferência pode variar, dependendo do número de registos.
- Se ocorrer um erro enquanto o ficheiro CSV estiver a ser transferido ou criado, a transferência é cancelada e os detalhes sobre o erro são incluídos no final do ficheiro.
- Se um registo for transferido com sucesso, aparecerá "Download completed." na última linha do ficheiro de registo.
- Para mais informações sobre guardar ficheiros de registo CSV, consulte a Ajuda do seu browser.
- Os ficheiros de registo transferidos utilizam a codificação UTF-8. Para visualizar um ficheiro de registo, abra-o utilizando uma aplicação que suporte UTF-8.
- Para mais informações sobre os itens contidos nos registos, consulte Pág. 185 "Atributos dos registos que é possível transferir".

Número de registos que podem ser mantidos no equipamento

Quando é excedido o limite de registos de trabalhos, registos de acessos ou registos ecológicos que podem ser mantidos no equipamento e são gerados novos registos, os registos antigos são substituídos pelos novos. Se os registos não forem transferidos periodicamente, poderá não ser possível guardar os registos antigos em ficheiros.

Quando utilizar o Web Image Monitor para gerir registos, transfira os registos a intervalos adequados às condições apresentadas na tabela.

Após transferir os registos, execute uma eliminação em grupo dos registos.

Se alterar a definição [Recolher] / [Não recolher] para a recolha de registos, deve executar uma eliminação agrupada dos registos.

Números máximos de registos que podem ser guardados no equipamento

Tipos de registo	Número máximo de registos
Registos de trabalhos	4000
Registos de acessos	12 000
Registos ecológicos	4000

Números estimados de registos criados por dia

Tipos de registo	Número de registos criados por dia
Registos de trabalhos	100
Registos de acessos	300 Este número é baseado em 100 operações, como operações de inicialização e acesso através da Web, e 200 entradas de registo de trabalhos (2 entradas por trabalho: 1 para o início de sessão e 1 para o encerramento da sessão).
Registos ecológicos	100

Nestas condições, o equipamento pode manter registos durante 40 dias sem substituição. É recomendada a transferência de registos a cada 20 dias em caso de erros.

O administrador do equipamento deve gerir os ficheiros de registos transferidos de forma apropriada.

Nota

- Durante a transferência de registos, não efetue operações que criem entradas de registos, uma vez que os registos que estão a ser transferidos não podem gravar novas entradas.
- A eliminação em grupo dos registos pode ser executada no painel de controlo ou através do Web Image Monitor.

Notas acerca do funcionamento quando o número de entradas de registo atinge o máximo

Se o número de registos que podem ser guardados no equipamento exceder o limite especificado, os registos mais antigos são apagados e substituídos pelos registos mais recentes. O número máximo de registos que é possível guardar é definido para cada registo de trabalhos, registo de acesso e registo ecológico.

O registo de trabalho e registo de acesso são transferidos como um só ficheiro.

"Se os registos forem transferidos sem substituição", abaixo, indica que o registo de trabalho e o registo de acesso são agregados após a transferência.

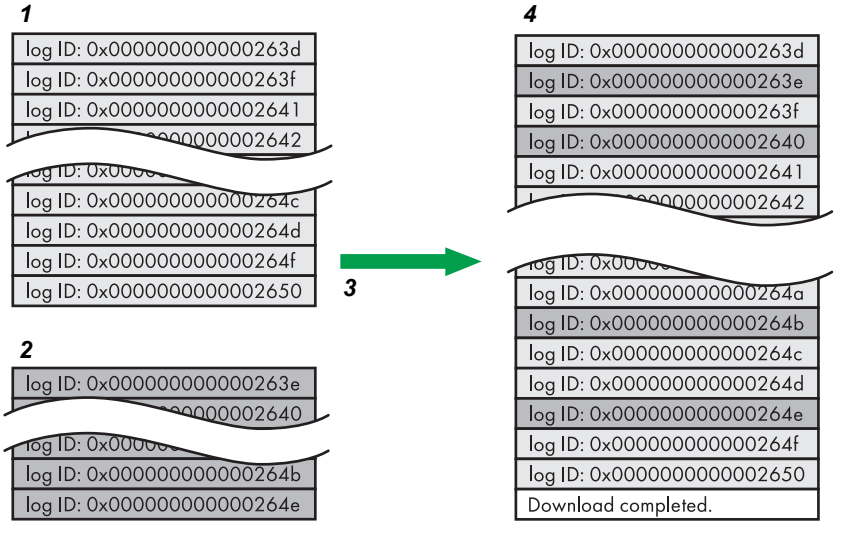
"Se os registos forem transferidos durante a substituição", abaixo, indica que parte do registo de acesso é substituído.

Neste exemplo, parte do registo de acesso foi substituído por um registo transferido e eliminado.

O registo ecológico é transferido como um ficheiro independente.

As entradas de registos são substituídas por ordem de prioridade. As entradas de registos com maior prioridade não serão substituídas ou apagadas.

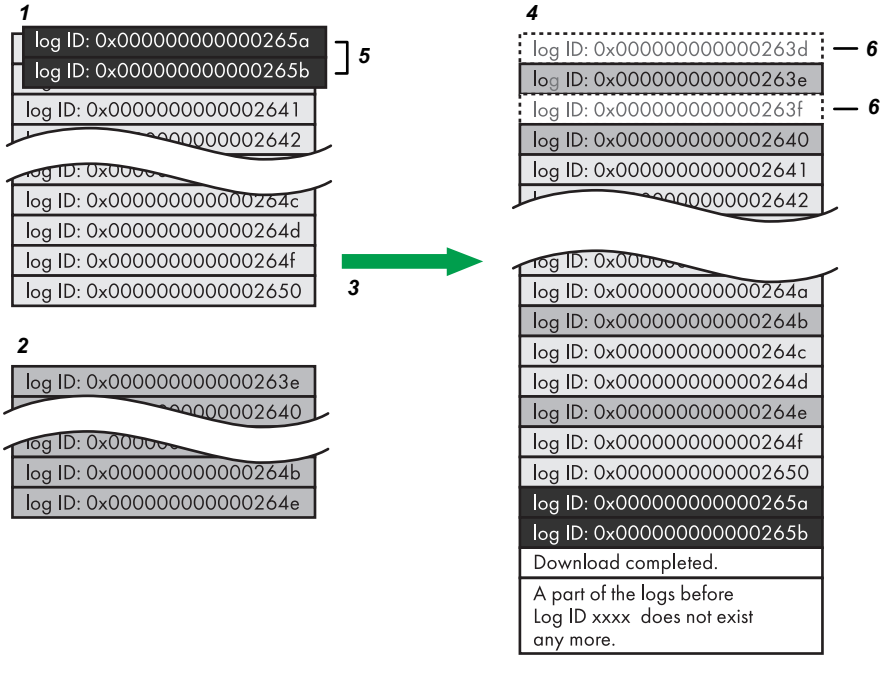
Se os registos forem transferidos sem substituição



CJD006

1. **Registo de acesso**
2. **Registo de trabalhos**
3. **Transferência**
4. **Registos transferidos**

se os registos forem transferidos durante a substituição



CJD007

1. **Registo de acesso**
2. **Registo de trabalhos**
3. **Transferência**
4. **Registos transferidos**
5. **Substituição**
6. **Apagados por substituição**

Para determinar se a substituição ocorreu ou não enquanto os registos estavam a ser transferidos, verifique a mensagem na última linha dos registos transferidos.

- Se a substituição não tiver ocorrido, na última linha estará presente a seguinte mensagem: Download completed.
- Se a substituição tiver ocorrido, a última linha irá conter a seguinte mensagem: Download completed. A part of the logs before Log ID xxxx does not exist any more.

Nota

- Em caso de substituição, parte dos registos terão sido eliminados pela substituição; como tal, verifique o registo "Log ID xxxx" e registos mais recentes.

Registos de trabalhos de impressora

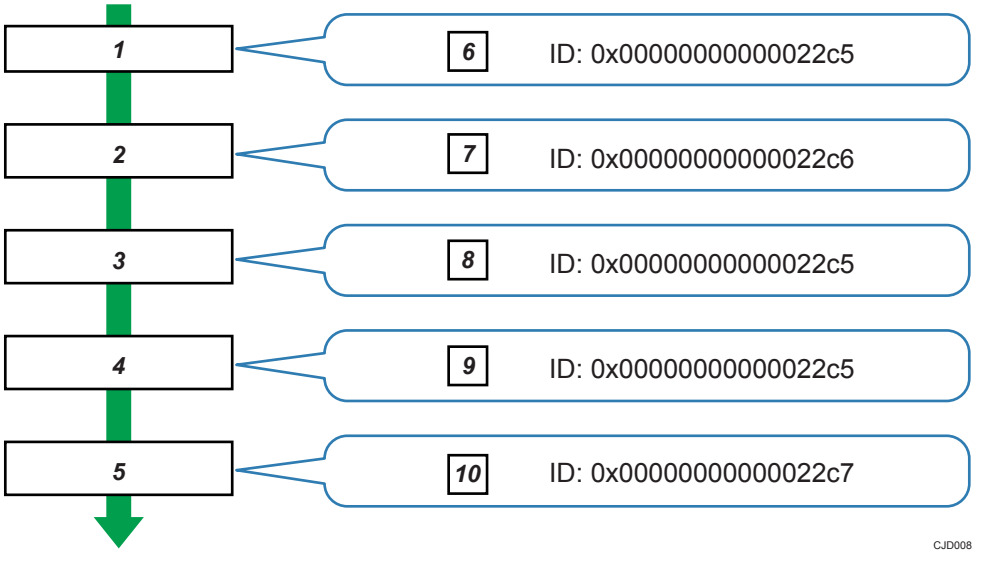
As entradas de registo de impressão são gravadas antes de a entrada de início de sessão ser gravada no registo de acessos.

Os detalhes de trabalhos (receção, processamento, saída de dados dos trabalhos, entre outros) são gravados como entradas individuais.

Quando o equipamento recebe um trabalho de impressão, cria uma ID para o trabalho e guarda-o no registo de trabalhos. O equipamento cria então uma ID de início de sessão para o trabalho de impressão e guarda-o no registo de acessos. Em seguida, cria uma entrada de registo de trabalho para detalhes do trabalho que é processado e exportado (com a mesma ID de início de sessão). Quando o equipamento concluir o processamento do trabalho, cria uma entrada de registo e coloca-a no registo de acessos.

As entradas com detalhes acerca de operações, como a receção, o processamento e a saída de trabalhos de impressão, são criadas primeiro no registo de trabalhos e, de seguida, os detalhes do início de sessão e encerramento da sessão são guardados no registo de acessos.

Diagrama de um trabalho de impressão



1. **Os dados do trabalho de impressão são recebidos.**
2. **Os dados de autenticação (início de sessão) são recebidos.**
3. **O trabalho de impressão é processado.**
4. **O trabalho de impressão é concluído.**
5. **Os dados de autenticação (início de sessão) são recebidos.**
6. **É atribuída uma ID ao trabalho de impressão que é guardado como uma entrada no registo de trabalhos.**
7. **Os dados de autenticação (início de sessão) são guardados como uma entrada no registo de acessos.**
8. **A informação acerca do processamento do trabalho de impressão é guardada como uma entrada no registo de trabalhos (utilizando a mesma ID).**
9. **A informação acerca da saída do trabalho de impressão é guardada como uma entrada no registo de trabalhos (utilizando a mesma ID).**
10. **Os dados de autenticação (encerramento da sessão) são guardados como uma entrada no registo de acessos.**

Eliminar todos os registos

Utilize o seguinte procedimento para eliminar todos os registos guardados no equipamento.

"Apagar todos os registos" surge se um dos registos de trabalhos, registos de acessos ou registos ecológicos está definido como [Ativo].

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Registos] sob "Definições do dispositivo".**
4. **Clique em [Apagar] em "Apagar todos os registos".**
5. **Clique em [OK].**
6. **Encerre sessão.**

Desativar a transferência de registos para o servidor de recolha de registos

Execute o procedimento seguinte para desativar a transferência de registos para o servidor de recolha de registos. Tenha em atenção que apenas pode mudar as definições da transferência dos registos para [Inativo] se já estiver definido como [Ativo].

1. **Inicie sessão como administrador do equipamento a partir do Web Image Monitor.**
2. **Aponte para [Gestão de equipamentos] e, em seguida, clique em [Configuração].**
3. **Clique em [Registos] sob "Definições do dispositivo".**
4. **Selecione [Inativo] na área [Transferir registos], em "Definições comuns para todos os registos".**
5. **Clique em [OK].**
6. **Encerre sessão.**

Gerir Registos a Partir do Equipamento

Pode especificar definições como a definição de recolha de registos, se os registos devem ou não ser transferidos para o servidor de recolha de registos e se todos os registos devem ou não ser apagados.

Especificar as definições da recolha de registos

Active as definições de recolha para cada tipo de registo.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 4 vezes.**
5. **Prima [Recolher registos].**
6. **Selecione [Ativo] para cada função: "Registo dos trabalhos", "Registo dos acessos" e "Registos ecológicos".**
7. **Prima [OK].**
8. **Encerre sessão.**
9. **Desligue o interruptor de alimentação e, em seguida, volte a ligá-lo.**

Desativar a transferência de registos para o servidor de recolha de registos

Utilize o procedimento seguinte para desativar a transferência de registos do equipamento para o servidor de recolha de registos. Note que pode mudar a definição da transferência do registo para [Desligado] apenas se estiver atualmente definido como [Ligado].

Para mais informações sobre o servidor de recolha de registos, contacte o revendedor local.

Para mais informações sobre a definição do registo de transferência, consulte a ajuda do servidor de recolha de registos.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] duas vezes.**
5. **Prima [Definição do registo de transferência].**
6. **Prima [Desligado].**
7. **Prima [OK].**
8. **Encerre sessão.**

Especificar Apagar todos os registos

Utilize o seguinte procedimento para eliminar todos os registos guardados no equipamento.

Apenas pode eliminar todos os registos do equipamento em lote se utilizar o servidor de recolha de registos ou tiver especificado a definição Web Image Monitor para recolher o registo de trabalhos, registo de acessos ou registo ecológico.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] duas vezes.**
5. **Prima [Apagar todos os registos].**
6. **Prima [Sim].**
7. **Prima [Sair].**
8. **Encerre sessão.**

Gerir registos a partir do servidor de recolha de registos

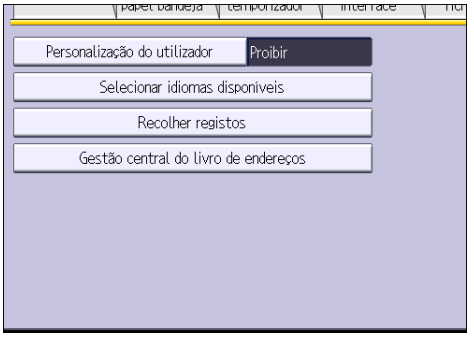
Para mais informações sobre como utilizar o servidor de recolha de registos para fazer a gestão dos ficheiros de registo, consulte o manual fornecido com o servidor de recolha de registos.

Configurar o Ecrã Inicial para Utilizadores Individuais

Isto permite que cada utilizador utilize o seu próprio ecrã inicial.

Quando um utilizador inicia sessão, é apresentado o respetivo ecrã inicial personalizado.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 4 vezes.**
5. **Prima [Personalização do utilizador].**



6. **Prima [Permitir], seguido de [OK].**
7. **Encerre sessão.**

Nota

- Isto também pode ser configurado a partir do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- As informações do ecrã inicial para cada utilizador são mantidas mesmo quando "Personalização do utilizador" está definido como [Proibir]. Quando a definição voltar a estar configurada como [Permitir], as informações podem ser utilizadas novamente.

Avisos sobre a utilização de ecrãs iniciais personalizados

Observe estes avisos antes de utilizar esta função.

- Quando um utilizador é registado no livro de endereços, é criado um ecrã inicial para esse utilizador. O ecrã inicial personalizado do utilizador é configurado com as predefinições (disposição dos ícones).

- Se Menu protegido for definido como [Nível 1] ou [Nível 2],o utilizador não poderá utilizar o registo de programas dessa função, editar ou eliminar o ecrã. No entanto, o utilizador pode adicionar ícones ao seu ecrã inicial.
- Se Menu protegido tiver sido definido como [Nível 1] ou [Nível 2], peça ao administrador do equipamento para criar os programas necessários.
- São visualizados apenas os ícones das funções que o utilizador tem permissão para utilizar.
- Quando um utilizador é eliminado do livro de endereços, as informações do ecrã inicial do utilizador são também eliminadas.
- Quando um utilizador edita um programa, as alterações são aplicadas aos ecrãs iniciais dos utilizadores que possuem o ícone do programa nos seus ecrãs iniciais.
- Quando um utilizador elimina um programa, o ícone do programa é eliminado de todos os ecrãs iniciais de todos os utilizadores que possuem o ícone do programa no respetivo ecrã inicial.
- Uma vez que cada utilizador pode personalizar o seu ecrã inicial, o administrador não pode verificar as informações do ecrã inicial de cada utilizador.

Configurar as Definições do Browser

Precauções para utilizar a função de browser

A comunicação entre o equipamento e o servidor através de um browser está exposta a ataques de escuta e manipulação de dados. Como tal, recomenda-se a instalação dos certificados externos emitidos para os websites aos quais o equipamento tem permissão para aceder e a ativação prévia da função de Verificar certificado a partir do site. O acesso não autorizado pode ser impedido se permitir ao equipamento aceder apenas a websites cujos certificados estejam instalados no equipamento.

É recomendado que ative [Verificar certificado a partir do site] especialmente quando enviar dados utilizando Extended JavaScript.

Para ativar [Verificar certificado a partir do site], é necessário ativar a função SSL do equipamento e instalar certificados de site.

Para mais informações sobre como configurar o SSL, consulte Pág. 112 "Configurar as Definições SSL/TLS".

Para mais informações sobre como instalar certificados externos, consulte Pág. 144 "Configurar a Autenticação IEEE 802.1X".

As definições do equipamento para Verificar certificado a partir do site podem ser especificadas apenas através do Web Image Monitor.

Consulte artigos relacionados na Ajuda do Web Image Monitor.

Se [Verificar certificado a partir do site] estiver desativado e o utilizador aceder a um website não fidedigno, poderá ser apresentada uma mensagem de aviso.

Nesse caso, o website relacionado poderá ter problemas de segurança. Neste caso, o administrador do equipamento deverá consultar Pág. 223 "Troubleshooting" e, em seguida, dar instruções aos utilizadores no sentido de tomarem as medidas apropriadas.

Além disso, mesmo que não seja apresentada uma mensagem dessas, para minimizar o risco de fuga de informações e de manipulação de dados, o administrador deverá dar instruções aos utilizadores para verificarem os certificados e os URLs de todos os websites ligados, para que seja possível impedir o acesso a websites não autorizados.

Web site não fidedigno

Um "website não fidedigno" é o seguinte:

- Não emite um certificado.
- Uma fonte desconhecida emite o certificado do site.
- O certificado do site expirou.

Troubleshooting

Se o website ligado tiver um problema de segurança, poderá ser apresentada uma mensagem.

Nesse caso, o administrador do equipamento tem obrigatoriamente de verificar a mensagem e dar instruções aos utilizadores para que tomem as medidas necessárias.

Mensagens

- "Este site tem um problema de segurança. O certificado expirou."
- "Este site tem um problema de segurança. O certificado de origem para verificação não existe."
- "Este site tem um problema de segurança. Não é possível proceder à verificação do servidor a ligar."
- "Este site tem um problema de segurança. Os subconteúdos http estão incluídos no site https."*1

*1 O website ligado contém dados não encriptados.

Gerir Informações do Equipamento

⚠CUIDADO

- Mantenha os SD cards ou dispositivos de memória flash USB fora do alcance das crianças. Se uma criança engolir acidentalmente um SD card ou um dispositivo de memória flash USB, consulte imediatamente um médico.

As informações do dispositivo do equipamento podem ser definidas por um administrador com privilégios para gerir equipamentos, utilizadores, redes e ficheiros.

As informações de dispositivo do equipamento podem ser exportadas para um dispositivo externo como um ficheiro de informações para configuração do dispositivo. Se importar para o equipamento um ficheiro de informações para configuração do dispositivo, pode utilizá-lo como ficheiro de cópia de segurança para repor as definições do dispositivo.

Além disso, gerir o ficheiro com informação das definições do dispositivo com o servidor do dispositivo gestor permite que o ficheiro com informação das definições do dispositivo seja importado periodicamente num momento especificado ou aquando do arranque do dispositivo.

Dados que podem ser importados e exportados

- Funções de Copiador/Servidor de Documentos
- Funções de Impressora
- Funções de Scanner
- Funções de Browser
- Programa (Serv.documentos)
- Programa (Copiador)
- Programa (Scanner)
- Defin. Web Image Monitor
- Definições Web Service
- Definições do Sistema

Dados que não podem ser importados nem exportados

- Algumas definições do sistema *1 *2

*1 A definição para a data, as definições que requerem certificados do dispositivo e as definições que necessitam de ser ajustadas em cada equipamento (por exemplo, ajustes de imagem) não podem ser importadas ou exportadas.

*2 Definições apenas para executar funções e definições apenas para visualização não podem ser importadas ou exportadas.

- Definições de Função Avançada
- Livro de endereços
- Programas (função de impressora)

- Carimbo do utilizador em Funções de copiador/servidor documentos
- Definições que podem ser especificadas através de telnet
- Dados relacionados com o @Remote
- Contadores
- Definições que apenas podem ser especificadas através do Web Image Monitor ou Web Service (por exemplo, Bonjour, definição SSDP)

Nota

- O formato do ficheiro para exportações é CSV.
- A configuração do dispositivo do equipamento que importa o ficheiro de informação de definições do dispositivo tem de ser igual ao do equipamento que exportou o ficheiro de informação de definições do dispositivo. Caso contrário, não é possível importar o ficheiro de informações das definições de dispositivo.
- A importação e exportação é possível entre equipamentos apenas se os seus modelos, região de utilização e as seguintes configurações do dispositivo coincidirem.
  - Bandeja de entrada
  - Bandeja de saída
- Se a configuração do dispositivo for alterada, exporte o ficheiro de informação das definições do dispositivo.
- Se existirem equipamentos com a mesma configuração de dispositivo, pode especificar as suas definições importando o mesmo ficheiro de definições do dispositivo.
- Se o ecrã inicial contém ficheiros de imagem JPG, estes também serão exportados.
- Enquanto um utilizador estiver a operar o equipamento, nada pode ser importado nem exportado enquanto o utilizador não completar a operação.
- Durante a exportação e importação, o equipamento não pode ser utilizado de outra forma.
- Para mais informações acerca do manuseamento do SD card, consulte Getting Started.
- Também pode utilizar o Web Image Monitor para configurar as definições de importação, exportação e do servidor.

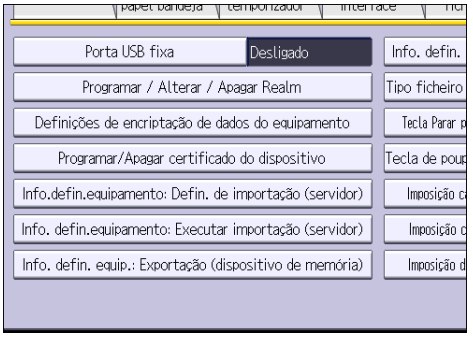
Exportar informações do equipamento

Quando as informações do equipamento são exportadas a partir do painel de controlo, os dados são guardados num SD card.

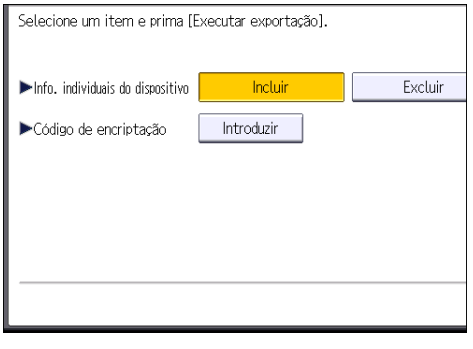
1. **Introduza um SD card no leitor de cartão de memória, na parte da frente do painel de controlo.**

   Para detalhes sobre como inserir o SD card, consulte Getting Started.

2. **Inicie sessão a partir do painel de controlo como administrador com privilégios de administrador de utilizadores, administrador de equipamento, administrador de rede e administrador de ficheiros.**
3. **Prima [Definições do sistema].**
4. **Prima [Ferr. Administrador].**
5. **Prima [▼Seg.] 3 vezes.**
6. **Prima [Info. defin. equip.: Exportação (dispositivo de memória)].**


Porta USB fixa
Desligado
Info. defin.
Programar / Alterar / Apagar Realm
Tipo ficheiro
Definições de encriptação de dados do equipamento
Programar/Apagar certificado do dispositivo
Info.defin.equipamento: Defin. de importação (servidor)
Info. defin.equipamento: Executar importação (servidor)
Info. defin. equip.: Exportação (dispositivo de memória)

7. **Defina as condições de exportação.**



- Selecione se pretende [Incluir] ou [Excluir] as "Info. individuais do dispositivo". As "Info. individuais do dispositivo" incluem o endereço IP, o nome de host, etc.
- Especifique uma chave de encriptação.

8. **Prima [Executar exportação].**
9. **Prima [OK].**
10. **Prima [Sair].**
11. **Encerre sessão.**

Nota

- Se a importação falhar, verifique o registo para identificar o erro. O registo é guardado na mesma localização do ficheiro de informação de definições do equipamento exportado.

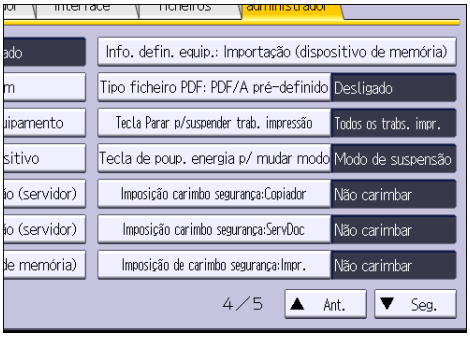
Importar informações do equipamento

Importe informações do equipamento guardadas num SD card.

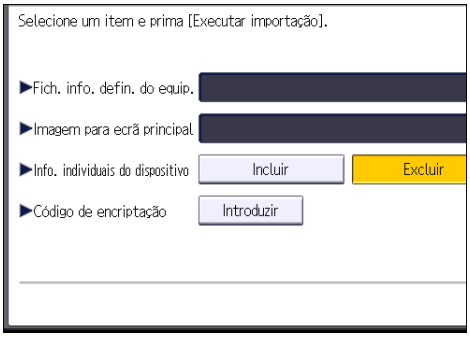
1. **Introduza um SD card no leitor de cartão de memória, na parte da frente do painel de controlo.**

   Para detalhes sobre como inserir o SD card, consulte Getting Started.

2. **Inicie sessão a partir do painel de controlo como administrador com privilégios de administrador de utilizadores, administrador de equipamento, administrador de rede e administrador de ficheiros.**
3. **Prima [Definições do sistema].**
4. **Prima [Ferr. Administrador].**
5. **Prima [▼Seg.] 3 vezes.**
6. **Prima [Info. defin. equip.: Importação (dispositivo de memória)].**



7. **Configure as condições da importação.**



- Prima [Selecionar] no "Fich. info. defin. do equip." para selecionar os ficheiros a importar.
- Ao adicionar uma imagem ao ecrã de início, prima [Selecionar] para "Imagem para ecrã principal" e, em seguida, selecione o ficheiro.
- Selecione se pretende [Incluir] ou [Excluir] as "Info. individuais do dispositivo". As "Info. individuais do dispositivo" incluem o endereço IP, o nome de host, etc.

- Introduza o código de encriptação especificado quando o ficheiro foi exportado.

8. **Prima [Executar importação].**
9. **Prima [OK].**
10. **Prima [Sair].**

    O equipamento é reiniciado.

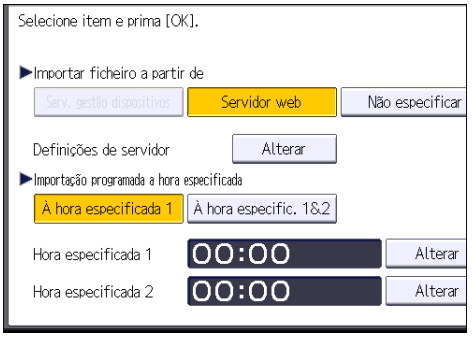
Nota

- Se a importação falhar, verifique o registo para identificar o erro. O registo é guardado na mesma localização do ficheiro de informação de definições do equipamento exportado.

Importar periodicamente informações do equipamento

Esta definição importa automaticamente para o equipamento as informações do dispositivo guardadas num servidor.

1. **Inicie sessão a partir do painel de controlo como administrador com privilégios de administrador de utilizadores, administrador de equipamento, administrador de rede e administrador de ficheiros.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Prima [Info.defin.equipamento: Definição de importação (servidor)].**
6. **Configure as condições da importação.**



- Selecione a fonte para importar ficheiros. Configure definições como URL, nome de utilizador, palavra-passe, etc., utilizando as definições de detalhes do servidor.
- Selecione a frequência para importar ficheiros de informações de definição do equipamento e defina o tempo utilizado para uma importação periódica com a frequência especificada.
- Selecione se pretende ou não importar um ficheiro com informações de definições do equipamento se for idêntico ao último ficheiro importado.

- Quando o ficheiro de informações das definições do equipamento a ser importado estiver encriptado, configure uma chave de encriptação.
- Selecione se pretende ou não enviar uma notificação por e-mail ao administrador do equipamento quando a importação não for bem sucedida.

7. **Prima [OK].**
8. **Encerre sessão.**

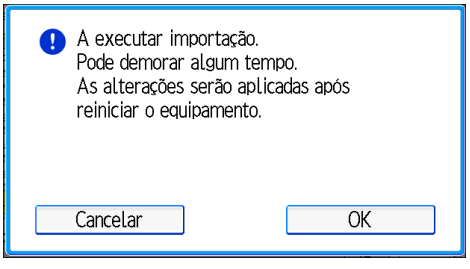
Nota

- Isto também pode ser configurado a partir do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- Quando é utilizado o servidor do dispositivo gestor, é possível especificar definições mais detalhadas para a importação. Para mais informações, consulte o manual do servidor do dispositivo gestor.
- Se a importação falhar, verifique o registo para identificar o erro. O registo é guardado na mesma localização do ficheiro de informação de definições do equipamento exportado.

Importar manualmente o ficheiro de informações das definições do equipamento a partir de um servidor

Importe manualmente para o equipamento o ficheiro de informações das definições do equipamento especificado com [Info.defin.equipamento: Definição de importação (servidor)].

1. **Inicie sessão a partir do painel de controlo como administrador com privilégios de administrador de utilizadores, administrador de equipamento, administrador de rede e administrador de ficheiros.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] 3 vezes.**
5. **Prima [Info. defin.equipamento: Executar importação (servidor)].**
6. **Prima [OK].**



7. **Prima [Sair].**

   O equipamento é reiniciado.

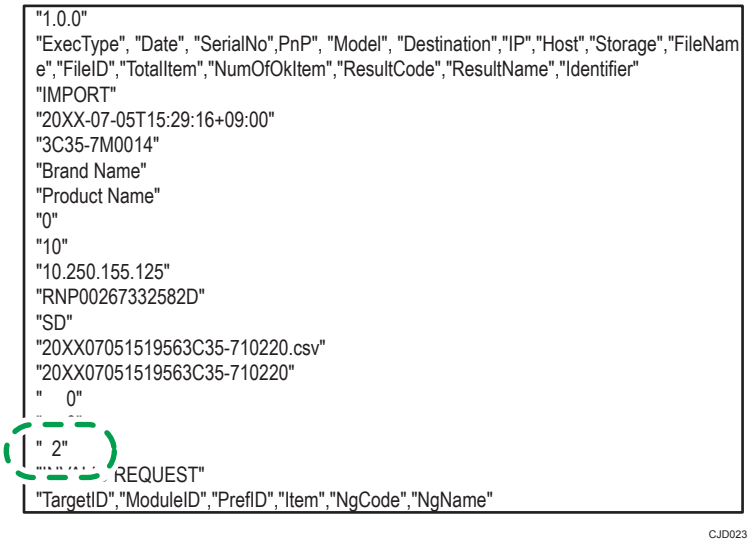
Nota

- Se a importação falhar, verifique o registo para identificar o erro. O registo é guardado na mesma localização do ficheiro de informação de definições do equipamento exportado.

Troubleshooting

Se ocorrer um erro, verifique primeiro o código de resultado do registo. Valores diferentes de 0 indicam a ocorrência de um erro. O código de resultado aparece na área com um círculo ilustrada abaixo.

Exemplo de um ficheiro de registo



CJD023

Se não conseguir resolver o problema ou não souber como resolvê-lo depois de verificar o código, anote os dados do registo de erro e contacte a assistência técnica.

ResultCode	Causa	Soluções
2 (INVALID REQUEST)	Foi tentada uma importação de ficheiro entre modelos diferentes ou equipamentos com diferentes configurações do dispositivo.	Importe ficheiros exportados a partir do mesmo modelo com a mesma configuração do dispositivo.

ResultCode	Causa	Soluções
4 (INVALID OUTPUT DIR)	Não foi possível escrever a informação de dispositivo no dispositivo de destino.	Verifique se o dispositivo de destino está a funcionar corretamente.
7(MODULE ERROR)	Ocorreu um erro inesperado durante uma importação ou exportação.	Desligue a alimentação e ligue-a novamente e, em seguida, tente executar a operação novamente. Se o erro persistir, contacte a assistência técnica.
8 (DISK FULL)	O espaço de armazenamento disponível no suporte externo é insuficiente.	Execute a operação novamente após certificar-se de que possui espaço suficiente.
9 (DEVICE ERROR)	A escrita ou leitura do ficheiro de registo falhou.	Verifique se o caminho para a pasta de armazenamento do ficheiro ou a pasta em que o ficheiro está guardado não está disponível.
10 (LOG ERROR)	Não foi possível escrever no ficheiro de registo. O disco rígido está danificado.	Contacte a assistência técnica.

ResultCode	Causa	Soluções
20 (PART FAILED)	A importação de algumas definições falhou.	O motivo da falha está gravado em "NgName". Verifique o código. **Motivo para erro (NgName)** 2 INVALID VALUE O valor especificado excede o intervalo permitido. 3 PERMISSION ERROR A permissão para editar a definição não está disponível. 4 NOT EXIST A definição não existe no sistema. 5 INTERLOCK ERROR A definição não pode ser alterada devido ao estado do sistema ou ao interbloqueio com outras definições especificadas. 6 OTHER ERROR A definição não pode ser alterada por outro motivo.
21 (INVALID FILE)	A importação do ficheiro falhou porque está num formato incorreto no suporte externo.	Verifique se o formato do ficheiro está correto. O registo está no formato de ficheiro CSV.
22 (INVALID KEY)	A chave de encriptação não é válida.	Utilize a chave de encriptação correta.

Gerir o Livro de Endereços

Especificar a eliminação automática de dados do livro de endereços

Especifique o modo como o equipamento processa um pedido de registo automático depois de os dados registados no livro de endereços atingirem o limite.

Se definir esta opção para [Ligado], as contas de novos utilizadores são adicionadas eliminando automaticamente contas de utilizadores antigos. As contas que não são utilizadas há mais tempo são eliminadas primeiro.

Se definir esta opção para [Desligado], as contas de utilizadores antigos não são eliminadas, pelo que não é possível adicionar contas de novos utilizadores quando o número de dados registados atingir o limite.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [Apagar auto utiliz. livro end.].**
5. **Selecione [Ligado] e prima [OK].**
6. **Encerre sessão.**

Nota

- Os dados são eliminados automaticamente apenas quando o equipamento recebe um pedido de registo de dados. Não é executada a eliminação automática se as contas de utilizador forem adicionadas manualmente.
- Apenas as contas de utilizadores com códigos de utilizador ou nomes de utilizador e palavras-passes de início de sessão serão eliminadas automaticamente.

Eliminar todos os dados do livro de endereços

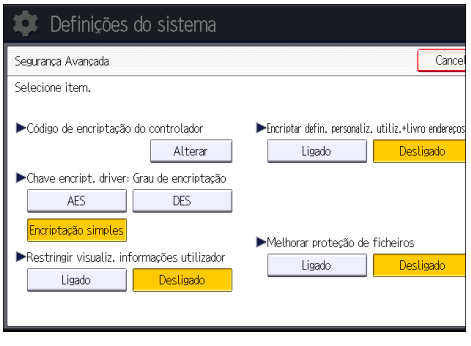
Pode eliminar todos os dados registados no livro de endereços.

1. **Inicie sessão como administrador de utilizadores no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [Apagar todos os dados no livro de endereços].**
5. **Prima [Sim], seguido de [Sair].**
6. **Encerre sessão.**

Especificar as Funções de Segurança Avançadas

Além de proporcionar segurança básica através da autenticação do utilizador e dos limites de acesso ao equipamento especificados por cada administrador, é possível aumentar a segurança encriptando os dados transmitidos e os dados no livro de endereços.

1. **Inicie sessão a partir do painel de controlo como administrador com privilégios.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.].**
5. **Prima [Segurança Avançada].**
6. **Prima a definição que pretende alterar e altere as definições.**



7. **Prima [OK].**
8. **Encerre sessão.**

Nota

- Os privilégios de operação de um administrador variam consoante a definição.

Código de encriptação do controlador

O administrador da rede pode especificar esta opção.

Especifique uma cadeia de texto para desencriptar palavras-passe de início de sessão ou palavras-passe de ficheiros enviadas a partir do driver quando a autenticação do utilizador estiver definida como ligada.

Para especificar uma chave de encriptação do driver, registe no driver a chave de encriptação especificada utilizando o equipamento no driver.

Para obter detalhes, consulte Pág. 151 "Especificar um código de encriptação do controlador".

Chave encript. driver: Grau de encriptação

O administrador da rede pode especificar esta opção.

Especifique o grau de encriptação para enviar trabalhos a partir do driver para o equipamento.

O equipamento verifica o grau de encriptação da palavra-passe anexada a um trabalho e processa-o.

Se for especificada [Encriptação simples], são aceites todos os trabalhos que são verificados por autenticação do utilizador.

Se for especificado [DES], são aceites trabalhos encriptados com DES ou AES.

Se for especificado [AES], são aceites trabalhos encriptados com AES.

Se selecionar [AES] ou [DES], especifique as definições de encriptação utilizando o driver de impressão. Para mais informações sobre como especificar o driver de impressão, consulte a Ajuda do mesmo.

Predefinição: [**Encriptação simples**]

Restringir visualiz. informações utilizador

O administrador do equipamento pode especificar esta opção se a autenticação do utilizador estiver especificada.

Quando o histórico de trabalhos é selecionado utilizando uma ligação de rede para a qual não exista autenticação, todas as informações pessoais podem ser visualizadas como "*********". Os utilizadores não autorizados são impedidos de obter informações acerca dos ficheiros registados, uma vez que não é possível visualizar as informações que identificam os utilizadores registados.

Predefinição: [**Desligado**]

Encriptar defin. personaliz. utiliz.+livro endereços

O administrador de utilizadores pode especificar esta opção.

Encripte as definições individuais dos utilizadores do equipamento e os dados no livro de endereços.

Mesmo que as informações internas do equipamento sejam obtidas ilegalmente, a encriptação impede que as definições individuais do utilizador ou que os dados do livro de endereços sejam lidos.

Para obter detalhes, consulte Pág. 73 "Proteger o Livro de Endereços".

Predefinição: [**Desligado**]

Melhorar proteção de ficheiros

O administrador do ficheiro pode especificar esta opção.

Ao especificar uma palavra-passe, o administrador de ficheiros pode limitar operações, como imprimir, eliminar e enviar ficheiros. Além disso, o administrador de ficheiros pode impedir que utilizadores não autorizados acedam aos ficheiros. Contudo, ainda é possível impedir que as palavras-passe sejam decifradas.

Ao especificar "Melhorar proteção de ficheiros", os ficheiros são bloqueados e tornam-se inacessíveis se uma palavra-passe inválida for introduzida dez vezes. Desta forma, é possível

proteger os ficheiros contra tentativas de acesso não autorizado utilizando palavras-passe aleatórias.

No caso de a função Melhorar proteção de ficheiros estar ativada, o ícone é apresentado no canto inferior direito do ecrã.

Os ficheiros bloqueados só podem ser desbloqueados pelo administrador de ficheiros.

Quando os ficheiros estão bloqueados, não é possível selecioná-los mesmo se for introduzida a palavra-passe correta.

Predefinição: [**Desligado**]

Restringir utilização de destinos

O administrador de utilizadores pode especificar esta opção.

Os destinos de scanner disponíveis estão limitados aos destinos registados no Livro de endereços.

Nenhum utilizador pode introduzir diretamente os destinos para transmissão.

Se especificar a definição de receber e-mails através de SMTP, não pode utilizar "Restringir utilização de destinos".

Podem ser utilizados os destinos procurados através de "Busca LDAP".

Para obter detalhes, consulte Pág. 65 "Restringir Uso da Lista de Destinos".

Predefinição: [**Desligado**]

Restringir adição de destinos utilizadores

O administrador de utilizadores pode especificar esta opção.

Se definir "Restringir adição de destinos utilizadores", os utilizadores poderão registar um destino de scanner no livro de endereços simplesmente introduzindo o destino e premindo [ProgDest]. Se definir estas funções como [Ligado], a tecla [ProgDest] não aparece. Apesar disto, os utilizadores poderão introduzir diretamente um destino utilizando o ecrã do scanner, mas não poderão registar esse destino no livro de endereços premindo [ProgDest].

Tenha igualmente em conta que, mesmo que defina estas funções como [Ligado], os utilizadores registados no livro de endereços podem alterar a respetiva palavra-passe. Apenas o administrador de utilizadores pode alterar outros itens que não sejam palavras-passe.

Predefinição: [**Desligado**]

Definições em SNMPv1, v2

O administrador da rede pode especificar esta opção.

Se forem utilizados os protocolos SNMPv1 ou SNMPv2 para aceder ao equipamento, a autenticação não pode ser efetuada para que as definições de papel ou outras definições especificadas pelo administrador do equipamento possam ser alteradas. Se selecionar [Proibir], a definição pode ser visualizada mas não especificada com SNMPv1, v2.

Predefinição: [**Não proibir**]

Autenticar trabalho atual

O administrador do equipamento pode especificar esta opção.

Esta definição permite especificar se a autenticação é necessária ou não para operações, como cancelar trabalhos nas funções de copiador e impressora.

Se selecionar [PrivilégioInícioSessão], podem utilizar o equipamento os utilizadores autorizados e o administrador do equipamento. Quando esta opção é selecionada, não é necessária autenticação dos utilizadores que tenham iniciado sessão no equipamento antes de ter sido selecionado o [PrivilégioInícioSessão].

Se [PrivilégioAcesso] estiver especificado, qualquer utilizador que tenha feito um trabalho de impressão ou de cópia pode cancelar o trabalho. Também o administrador do equipamento pode cancelar o trabalho de cópia ou de impressão do utilizador.

Mesmo que tenha selecionado [PrivilégioInícioSessão] e iniciado sessão no equipamento, não pode cancelar um trabalho de cópia ou de impressão em curso se não tiver privilégios para utilizar as funções de cópia e impressora.

Só pode especificar "Autenticar trabalho atual" se tiver sido especificada a Gestão de autenticação do utilizador.

Predefinição: [**Desligado**]

Política da palavra-passe

O administrador de utilizadores pode especificar esta opção.

Esta definição permite-lhe especificar [Definição Complexidade] e [Nº mínimo de carateres] para a palavra-passe. Especificando esta definição, apenas pode utilizar palavras-passe que cumpram as condições especificadas em "Definição Complexidade" e em "Nº mínimo de carateres".

Se selecionar [Nível 1], especifique a palavra-passe utilizando uma combinação de 2 tipos de carateres selecionados entre letras maiúsculas, letras minúsculas, números decimais e símbolos como #.

Se selecionar [Nível 2], especifique a palavra-passe utilizando uma combinação de 3 tipos de carateres selecionados entre letras maiúsculas, letras minúsculas, números decimais e símbolos como #.

Predefinição: [**Desligado**]. Não existem restrições relativamente ao número de carateres e os tipos de carateres não são especificados.

@Remote Service

O administrador do equipamento pode especificar esta opção.

A comunicação através de HTTPS para o @Remote Service fica desativada se selecionar [Proibir].

Quando a definir como [Proibir], contacte a assistência técnica.

Se estiver definido para [Proibir alguns serviços], torna-se impossível alterar definições a partir de uma ligação remota, o que proporciona uma operação bastante mais segura.

Predefinição: [**Não proibir**]

Atualizar firmware

O administrador do equipamento pode especificar esta opção.

Esta definição permite especificar se são permitidas ou não atualizações de firmware no equipamento. Um técnico de assistência atualiza o firmware ou as atualizações de firmware são efetuadas através da rede.

Se selecionar [Proibir], o firmware do equipamento não será atualizado.

Se selecionar [Não proibir], não existem restrições nas atualizações de firmware.

Predefinição: [**Não proibir**]

Alterar estrutura do firmware

O administrador do equipamento pode especificar esta opção.

Esta definição permite especificar se devem ser impedidas alterações na estrutura do firmware do equipamento. A função de Alterar Estrutura do Firmware deteta o estado do equipamento quando o SD card é inserido, removido ou substituído.

Se selecionar [Proibir], o equipamento para durante o arranque se for detetada uma alteração da estrutura do firmware e aparece uma mensagem solicitando o início de sessão do administrador. Depois de o administrador do equipamento iniciar sessão, o equipamento termina o arranque com o firmware atualizado.

O administrador pode verificar se a alteração de estrutura atualizada é permitida ou não, verificando a versão do firmware visualizada no ecrã do painel de controlo. Se a alteração da estrutura do firmware não for permitida, contacte o seu representante de assistência técnica antes de iniciar a sessão.

Se "Alterar estrutura do firmware" for definido como [Proibir], é necessário ativar a autenticação de administrador.

Após especificar [Proibir], desative a autenticação do administrador. Quando a autenticação do administrador for novamente ativada, pode repor a definição para [Não proibir].

Se selecionar [Não proibir], a alteração da estrutura do firmware é desativada.

Predefinição: [**Não proibir**]

Violação da introdução de palavra-passe

O administrador do equipamento pode especificar esta opção.

Se o número de pedidos de autenticação exceder o número especificado pela definição, o sistema reconhece o acesso como um ataque de palavras-passe. O acesso é guardado no registo de acessos e os dados do registo são enviados para o administrador do equipamento por e-mail.

Se "N.º máx. tentativas de acesso" estiver definido como [0], os ataques de palavras-passe não são detetados.

- N.º máx. tentativas de acesso

  Especifique o número máximo de tentativas de autenticação permitido.

Utilize as teclas numéricas para especificar o valor entre "0" e "100" e, em seguida, prima [#].

Predefinição: [30]

- Período de tempo

  Especifique o intervalo entre tentativas repetidas de autenticação que provocam falhas de autenticação. Quando o período de tempo terminar, os registos de tentativas de autenticação são apagados.

  Utilize as teclas numéricas para especificar o valor entre "1" e "10" e, em seguida, prima [#].

  Predefinição: [5]

Nota

- Dependendo dos valores especificados nas definições para [N.º máx. tentativas de acesso] e [Período de tempo], pode receber frequentemente e-mails de deteção de violações.
- Se receber frequentemente e-mails de deteção de violações, verifique o conteúdo e reveja os valores de definição.

Definição de segurança em caso de violação do acesso

O administrador do equipamento.

Quando iniciar sessão no equipamento através de uma aplicação de rede, um utilizador pode ficar bloqueado erradamente porque o número de tentativas de autenticação do utilizador não corresponde ao número de tentativas especificadas no equipamento.

Por exemplo, o acesso pode ser negado quando um trabalho de impressão para vários conjuntos de páginas é enviado a partir de uma aplicação.

Se selecionar [Ligado] sob "Definição de segurança em caso de violação do acesso", é possível evitar tais erros de autenticação.

- Ligado
  - DuraçãoBloqPorViolaçãoAcesso

    Especifique o número permitido de acessos do utilizador.

    Utilize as teclas numéricas para especificar o valor entre "0" e "60" e, em seguida, prima [#].

    Predefinição: [15]
  - LimitUtilizGeridosPeloHost

    Especifique o número de contas de utilizador que podem ser geridas na "Definição de segurança em caso de violação do acesso".

    Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, prima [#].

    Predefinição: [200]

- LimitP-PasseGeridasPeloHost

  Especifique o número de palavras-passes que podem ser geridas em "Definição de segurança em caso de violação do acesso".

  Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, prima [#].

  Predefinição: [200]

- Intervalo monitoriz estado

  Especifique o intervalo de monitorização de "LimitUtilizGeridosPeloHost" e "LimitP--PasseGeridasPeloHost".

  Utilize as teclas numéricas para especificar o valor entre "1" e "10" e, em seguida, prima [#].

  Predefinição: [3]

- Desligado

Predefinição: [**Desligado**]

Violação do acesso ao dispositivo

O administrador do equipamento pode especificar esta opção.

Se o número de pedidos de início de sessão exceder o número especificado pela definição, o sistema reconhece o acesso como uma violação de acesso. O acesso é guardado no registo de acessos e os dados do registo são enviados para o administrador do equipamento por e-mail. Além disso, é apresentada uma mensagem no painel de controlo e no Web Image Monitor.

Se "N.º máx. tentativas de acesso" estiver definido como [0], as violações de acesso não são detetadas.

Em "Tempo de atraso p/autenticação", é possível especificar o tempo de atraso para resposta aos pedidos de início de sessão para evitar que o sistema fique sem resposta quando é detetada uma violação de acesso.

Em "LimitAcessSimultGeridosPeloHost", é possível especificar o número máximo de hosts que acedem ao equipamento de uma só vez. Se o número de acessos simultâneos exceder o número especificado pela definição, a monitorização fica indisponível e o estado de monitorização do equipamento é guardado no registo.

- N.º máx. tentativas de acesso

  Especifique o número máximo de tentativas de acesso permitido.

  Utilize as teclas numéricas para especificar o valor entre "0" e "500" e, em seguida, prima [#].

  Predefinição: [100]

- Período de tempo

  Especifique o intervalo entre acessos excessivos. Quando terminar o período de tempo, os registos de acessos excessivos são apagados.

Utilize as teclas numéricas para especificar o valor entre "10" e "30" e, em seguida, prima [#].

Predefinição: [10]

- Tempo de atraso p/autenticação

  Especifique o tempo de atraso para autenticação quando é detetada uma violação de acesso.

  Utilize as teclas numéricas para especificar o valor entre "0" e "9" e, em seguida, prima [#].

  Predefinição: [3]

- LimitAcessSimultGeridosPeloHost

  Especifique o número de tentativas de autenticação aceitável quando as autenticações são atrasadas devido a uma violação de acesso.

  Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, prima [#].

  Predefinição: [200]

Nota

- Dependendo dos valores especificados nas definições para [N.º máx. tentativas de acesso] e [Período de tempo], pode receber frequentemente e-mails de deteção de violações.
- Se receber frequentemente e-mails de deteção de violações, verifique o conteúdo e reveja os valores de definição.

Outras Funções de Segurança

Esta secção explica as definições para impedir a fuga de informações.

São também explicadas as funções que ficam restringidas quando é ativada a autenticação de utilizador.

Função de Scanner

Imprimir e apagar jornal do scanner

Quando a autenticação do utilizador está ativada, "Imprimir e apagar jornal do scanner" é automaticamente definido para [Não imprimir: Desativ.envio] de modo a impedir que informações pessoais no histórico de transmissões/entregas sejam automaticamente impressas. Neste caso, o scanner é desativado automaticamente quando o histórico do jornal exceder 250 transmissões/entregas. Quando tal acontecer, selecione [Imprimir jornal do scanner] ou [Apagar jornal do scanner]. Para imprimir automaticamente o jornal do scanner, defina [Imprimir e apagar tudo] para "Imprimir e apagar jornal do scanner".

Para mais informações, consulte Scan.

Estado do sistema

Premir [Verificar estado] no painel de controlo permite-lhe verificar o estado atual do equipamento e as definições. Se a autenticação de administrador tiver sido especificada, [Info.EndereçosEquip.] apenas é apresentado em [Manut./Info./Equip.] se iniciou sessão na impressora como administrador.

Verificar a validade do firmware

Quando o equipamento é iniciado, esta função é utilizada para verficar se o firmware é válido.

Se ocorrer um erro durante o processo de verificação, é visualizado um erro de verificação no painel de controlo.

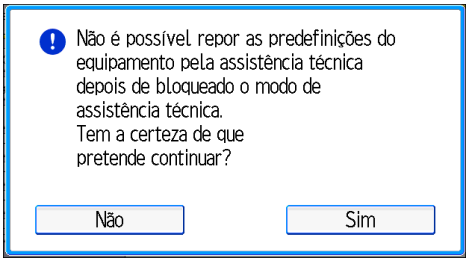
Note que isto também pode ser verificado no Web Image Monitor após o arranque do equipamento. Se ocorrer um erro durante um processo de verificação do Web Image Monitor, o Web Image Monitor não pode ser utilizado. Nesse caso, verifique o painel de controlo.

Restringir a Utilização por Parte de um Técnico de Assistência

É possível restringir o acesso do técnico do cliente ao modo de assistência técnica.

Um técnico do cliente utiliza um modo de assistência técnica para inspeção ou reparação. Se definir "Bloquear modo de assistência técnica" como [Ligado], o modo de assistência técnica apenas pode ser utilizado se o administrador do equipamento iniciar sessão no equipamento e cancelar o bloqueio do modo de assistência técnica, a fim de permitir que um técnico opere o equipamento para realizar trabalhos de inspeção e reparação. Isto garante que a inspeção e a reparação podem ser efetuadas sob a supervisão do administrador do equipamento.

1. **Inicie sessão como administrador do equipamento no painel de controlo.**
2. **Prima [Definições do sistema].**
3. **Prima [Ferr. Administrador].**
4. **Prima [▼Seg.] duas vezes.**
5. **Prima [Bloquear modo assistência técnica].**
6. **Prima [Ligado] e, em seguida, prima [OK].**
7. **Prima [Sim].**


Não é possível repor as predefinições do equipamento pela assistência técnica depois de bloqueado o modo de assistência técnica.
Tem a certeza de que pretende continuar?
Não
Sim

8. **Encerre sessão.**

Informações Adicionais para Segurança Avançada

Esta secção explica as definições que pode configurar para reforçar a segurança do equipamento.

Definições que pode configurar utilizando o painel de controlo

Utilize o painel de controlo para configurar as definições de segurança indicadas na seguinte tabela.

Definições do Sistema

Separador	Item	Definição
Defin. temporiz.	Temp. Encerramento Auto Sessão	Ligado: 180 segundos ou menos. Consulte Pág. 61 "Encerramento Automático de Sessão".
Ferr. Administrador	Gestão de autenticação de utilizador	Selecione [Autentic. básica] e defina "Autent. trab. impressora" para [Na totalidade]. Consulte Pág. 34 "Autenticação Básica".
Ferr. Administrador	Gestão de autenticação do administrador→Gestão de utilizadores	Selecione [Ligado] e selecione [Ferr. Administrador] para "Definições disponíveis". Consulte Pág. 13 "Configurar a Autenticação dos Administradores".
Ferr. Administrador	Gestão de autenticação do administrador→Gestão do equipamento	Selecione [Ligado] e, em seguida, cada uma das "Definições disponíveis". Consulte Pág. 13 "Configurar a Autenticação dos Administradores".
Ferr. Administrador	Gestão de autenticação do administrador→Gestão de rede	Selecione [Ligado] e selecione [Defin. interface], [Transfer. ficheiros] e [Ferr. Administrador] para "Definições disponíveis". Consulte Pág. 13 "Configurar a Autenticação dos Administradores".
Ferr. Administrador	Gestão de autenticação do administrador→Gestão de ficheiros	Selecione [Ligado] e selecione [Ferr. Administrador] para "Definições disponíveis". Consulte Pág. 13 "Configurar a Autenticação dos Administradores".

Separador	Item	Definição
Ferr. Administrador	Segurança Avançada→ Definições em SNMPv1, v2	Proibir Consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".
Ferr. Administrador	Segurança Avançada→ Chave encript. driver: Grau de encriptação	AES Consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".
Ferr. Administrador	Segurança Avançada→ Autenticar trabalho atual	PrivilégioAcesso Consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".
Ferr. Administrador	Segurança Avançada→ Política da palavra-passe	"Definição Complexidade": Nível 1 ou superior, "Nº mínimo de carateres": 8 ou superior Consulte Pág. 234 "Especificar as Funções de Segurança Avançadas".
Ferr. Administrador	Nível de segurança da rede	Nível 2 Para obter o estado do equipamento através do driver de impressão ou do Web Image Monitor, ative "SNMP" no Web Image Monitor. Consulte Pág. 102 "Especificar Níveis de Segurança da Rede".
Ferr. Administrador	Bloquear modo assistência técnica	Ligado Consulte Pág. 243 "Restringir a Utilização por Parte de um Técnico de Assistência".
Ferr. Administrador	Definições de encriptação de dados do equipamento	Selecione [Encriptar] e defina [Todos os dados] para "Transponha todos os dados ou apenas os dados do sistema de ficheiros (sem formatação) ou formate todos os dados.". Se [Encriptar] já tiver sido selecionado, não são necessárias mais definições de encriptação. Consulte Pág. 77 "Encriptar Dados no Equipamento".

Funções de Scanner

Separador	Item	Definição
Definições Iniciais	Menu protegido	Nível 2 Consulte Pág. 68 "Especificar a Função de Menu Protegido".

Nota

- A definição SNMP pode ser especificada em [SNMP] sobre [Configuração] no Web Image Monitor.

Definições que pode configurar utilizando o Web Image Monitor

Utilize o Web Image Monitor para configurar as definições de segurança apresentadas na tabela seguinte.

Gestão de equipamentos→Configuração

Categoria	Item	Definição
Definições do dispositivo→ Registos	Recolher registos de trabalhos	Ativo
Definições do dispositivo→ Registos	Recolher registos de acesso	Ativo
Segurança→ Política de bloqueio de utilizador	Bloqueio	Ativo Para obter detalhes, consulte Pág. 58 "Função de Bloqueio de Utilizadores".
Segurança→ Política de bloqueio de utilizador	Número de tentativas antes de bloquear	5 vezes ou menos. Para obter detalhes, consulte Pág. 58 "Função de Bloqueio de Utilizadores".

Categoria	Item	Definição
Segurança→ Política de bloqueio de utilizador	Temporizador de bloqueio de conta	Defina para [Ativo] ou [Inativo]. Quando definir para [Ativo], defina o temporizador de bloqueio de conta para 60 minutos ou mais. Para obter detalhes, consulte Pág. 58 "Função de Bloqueio de Utilizadores".
Segurança→ Política de bloqueio de utilizador	Bloquear utilizador durante	Quando definir "Temporizador de bloqueio de conta" como [Ativo], defina o temporizador de bloqueio de conta para 60 minutos ou mais. Para obter detalhes, consulte Pág. 58 "Função de Bloqueio de Utilizadores".
Rede→SNMPv3	Função SNMPv3	Inativo Para utilizar as funções SNMPv3, defina "Função SNMPv3" como [Ativo] e defina Permitir comunicação SNMPv3 como [Só encriptação]. Uma vez que SNMPv3 garante a autenticação para cada pacote, o Registo de Início de Sessão será desativado desde que SNMPv3 esteja ativo.
Segurança→ Segurança da rede	FTP	Inativo Antes de especificar esta definição, defina "Nível de segurança da rede" para [Nível 2] no painel de controlo.
Segurança	S/MIME	"Algoritmo de encriptação": AES de 128 bits, AES de 256 bits ou 3DES-168 bit Tem de registar o certificado do utilizador para utilizar o S/MIME.

Gestão de equipamentos

Categoria	Item	Definição
Livro de endereços→ Introdução detalhada→ Adicionar utilizador/Alterar →E-mail	Certificado do utilizador	Tem de registar o certificado do utilizador para utilizar o S/MIME.

Nota

- O administrador tem de indicar qual o nível que poderá ser especificado para o algoritmo de encriptação.
- Para mais informações sobre como especificar um algoritmo de encriptação e registar um certificado de utilizador, consulte Pág. 118 "Configurar S/MIME".

Definições que pode configurar quando o IPsec está disponível/indisponível

Toda a comunicação de e para equipamentos onde o IPsec está ativo é encriptada.

Se a sua rede suportar IPsec, recomendamos que a ative.

Definições que pode configurar quando o IPsec está disponível

Se o IPsec estiver disponível, configure as definições indicadas na tabela seguinte para melhorar a segurança dos dados que circulam na sua rede.

Definições do painel de controlo

Definições do Sistema

Separador	Item	Definição
Defin. interface	IPsec	Ativo
Defin. interface	Permitir comunicação SSL/TLS	Só texto cifrado

Definições do Web Image Monitor

Gestão de equipamentos→Configuração

Categoria	Item	Definição
Segurança→ IPsec→ Definições da chave de encriptação negociada automaticamente	Editar→Nível de segurança	Autenticação e elevada encriptação

Definições que pode configurar quando o IPsec não está disponível

Se o IPsec não estiver disponível, configure as definições apresentadas na tabela seguinte para melhorar a segurança dos dados que circulam na sua rede.

Definições do painel de controlo

Definições do Sistema

Separador	Item	Definição
Defin. interface	IPsec	Inativo
Defin. interface	Permitir comunicação SSL/ TLS	Só texto cifrado

Nota

- É possível definir "IPsec" e "Permitir comunicação SSL/TLS" utilizando o Web Image Monitor.

Proteger dados quando o IPsec não está disponível

Os seguintes procedimentos melhoram a segurança dos dados do utilizador quando o IPsec não está disponível.

Os administradores têm de fornecer instruções aos utilizadores para que estes realizem estes procedimentos.

Impressora

- Imprimir com protocolos que suportam encriptação:

  Para utilizar as funções de impressora, especifique sftp como o protocolo ou especifique IPP e ative SSL/TLS.

  Para mais informações sobre as definições de IPP, consulte o Driver Installation Guide.

Para mais informações sobre definições SSL/TLS, consulte Pág. 112 "Configurar as Definições SSL/TLS".

Scanner

- Enviar o endereço URL de ficheiros guardados

  Envie os URLs dos ficheiros digitalizados para os destinos, configurando [Definições de envio] em [Funções de scanner], em vez de enviar os ficheiros digitalizados propriamente ditos. Para mais informações, consulte Digitalização.

- Gerir ficheiros de digitalização utilizando o Web Image Monitor

  Utilize o Web Image Monitor através da sua rede para visualizar, apagar, enviar e transferir ficheiros digitalizados.

- Função de autenticação S/MIME

  Quando enviar ficheiros digitalizados anexados a e-mail, proteja-os aplicando um certificado S/MIME. Para isso, configure as definições de "Segurança" antes de enviar os ficheiros. Para detalhes sobre como enviar e-mail a partir do scanner, consulte Scan.

Nota

- Para mais informações sobre a ativação e desativação do IPsec utilizando o painel de controlo, consulte Connecting the Machine/ System Settings.
- Para mais informações sobre como especificar a definição do IPsec através do Web Image Monitor, consulte Pág. 125 "Configurar Definições IPsec".

8. Resolução de Problemas

Este capítulo descreve o que fazer se o equipamento não funcionar corretamente.

Se for Visualizada uma Mensagem

Este capítulo explica como tratar de problemas se uma mensagem aparecer no ecrã durante a autenticação do utilizador.

Se for apresentada uma mensagem diferente das que são apresentadas abaixo, siga a mensagem para resolver o problema.

"Não possui privilégios para utilizar esta função."

Os privilégios para utilizar a função não estão especificados.

Se esta mensagem aparecer quando utiliza uma função:

- A função não está especificada na definição de gestão do livro de endereços.
- O administrador de utilizadores tem de decidir se irá atribuir os privilégios adicionais para utilizar a função.

Se esta mensagem aparecer quando especifica uma definição do equipamento:

- O administrador varia dependendo das definições do equipamento que os utilizadores pretendem especificar.
- Utilizando a lista de definições, o administrador responsável pelas definições do equipamento que os utilizadores pretendem especificar tem de decidir se atribuem ou não os privilégios para a utilização da função.

"A autenticação falhou. Para iniciar sessão"

As causas de falhas de autenticação variam e são indicadas por códigos de erro.

Para obter detalhes, consulte Pág. 253 "Se Aparecer um Código de Erro".

"A Autenticação do Administrador para Gestão do Utilizador tem de ser definida antes de se poder efetuar esta seleção."

Os privilégios de administrador de utilizadores não foram ativados em [Gestão de autenticação do administrador].

- Para especificar a autenticação básica, a autenticação Windows ou a autenticação LDAP, é necessário ativar primeiro os privilégios do administrador de utilizadores em [Gestão de autenticação do administrador].

Para obter detalhes, consulte Pág. 13 "Configurar a Autenticação dos Administradores".

"Os ficheiros selecionados contêm ficheiros sem privilégios de acesso. Só os ficheiros com privilégios de acesso serão apagados."

Tentou apagar ficheiros sem possuir os privilégios necessários.

- O proprietário ou o administrador de ficheiros pode eliminar ficheiros. Para apagar um ficheiro para o qual não possui os privilégios necessários, contacte o proprietário ou o administrador de ficheiros.

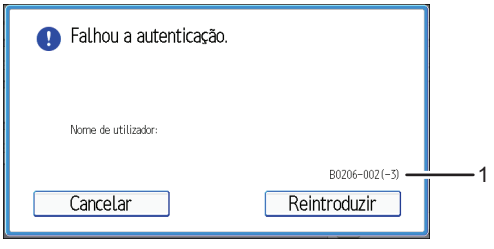
Nota

- Se aparecer uma mensagem de chamada de assistência técnica, contacte a assistência técnica.

Se Aparecer um Código de Erro

Se a autenticação falhar, aparece a mensagem "A autenticação falhou. Para iniciar sessão" com um código de erro. As listas seguintes fornecem soluções para cada código de erro. Se um código de erro não for apresentado nas listas abaixo, anote o código de erro e contacte a assistência técnica.

Posição do código de erro no visor



PT CJD014

1. **Código de erro**

   Aparece um código de erro.

Autenticação básica

B0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador iniciou sessão no equipamento e, em seguida, tente novamente.

B0104-000

Não foi possível desencriptar a palavra-passe.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida corretamente.
- [DES] ou [AES] é selecionado para "Chave de encriptação do driver: Grau de encriptação".

  Pode aceder especificando o código de encriptação do driver.
- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está corretamente especificado no driver.

B0206-002 : Caso 1

Ocorreu um erro com o nome de utilizador ou a palavra-passe de início de sessão.

- Certifique-se de que o nome de utilizador e a palavra-passe de início de sessão estão introduzidos corretamente e, em seguida, inicie a sessão.

B0206-002 : Caso 2

O utilizador tentou a autenticação a partir de uma aplicação no ecrã das "Definições do sistema", onde apenas o administrador possui privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

B0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes carateres proibidos.
- Se o nome da conta foi introduzido incorretamente, introduza-o corretamente e volte a iniciar a sessão.

B0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

B0208-000 / B0208-002

A conta está bloqueada porque o número de tentativas de autenticação permitidas atingiu o limite.

- Peça ao administrador de utilizadores para desbloquear a conta.

Autenticação Windows

W0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador possui sessão iniciada no equipamento e, em seguida, tente novamente.

W0104-000

Não foi possível encriptar uma palavra-passe.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida corretamente.
- [DES] ou [AES] é selecionado para "Chave de encriptação do driver: Grau de encriptação".

  Pode aceder especificando o código de encriptação do driver.
- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está corretamente especificado no driver.

W0206-002

O utilizador tentou a autenticação a partir de uma aplicação no ecrã das "Definições do sistema", onde apenas o administrador possui privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

W0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes carateres proibidos.
- Se o nome da conta foi introduzido incorretamente, introduza-o corretamente e volte a iniciar a sessão.

W0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

W0208-000 / W0208-002

A conta está bloqueada porque o número de tentativas de autenticação permitidas atingiu o limite.

- Peça ao administrador de utilizadores para desbloquear a conta.

W0400-102

A autenticação Kerberos falhou porque o servidor não está a funcionar corretamente.

- Certifique-se de que o servidor está a funcionar adequadamente.

W0400-200

Devido ao número significativo de tentativas de autenticação, todos os recursos estão ocupados.

- Aguarde alguns minutos e volte a tentar.

W0400-202: Caso 1

As definições SSL no servidor de autenticação e no equipamento não correspondem.

- Certifique-se de que as definições SSL no servidor de autenticação e no equipamento correspondem.

W0400-202: Caso 2

O utilizador introduziu sAMAccountName no nome de utilizador para iniciar sessão.

- Se um utilizador introduzir sAMAccountName como nome de utilizador de início de sessão, o ldap_bind falha num ambiente de domínio/subdomínio. Ao invés, utilize o UserPrincipleName (UPN) como nome de início de sessão.

W0406-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes carateres proibidos.
- Se o nome da conta foi introduzido incorretamente, introduza-o corretamente e volte a iniciar a sessão.

W0406-101

A autenticação não pode ser concluída devido ao número significativo de tentativas de autenticação.

- Aguarde alguns minutos e volte a tentar.
- Se a situação não melhorar, certifique-se de que não está a ocorrer um ataque ao nível da autenticação.
- Notifique o administrador da mensagem do ecrã por e-mail e verifique o registo do sistema quanto a potenciais ataques ao nível da autenticação.

W0406-107 : Caso 1

O formato UserPrincipleName (UPN) (utilizador@nomedomínio.xxx.com) está a ser utilizado para o nome de utilizador de início de sessão.

- O grupo do utilizador não pode ser obtido se o formato NomePrincipalUtilizador (utilizador@nomedomínio.xxx.com) for utilizado.
- Utilize "NomeContasAM(utilizador)" para iniciar a sessão, porque esta conta permite obter o grupo do utilizador.

W0406-107 : Caso 2

As definições atuais não permitem a recuperação do grupo.

- Certifique-se de que o âmbito do grupo de utilizadores está definido como "Grupo Global" e que o tipo de grupo está definido como "Segurança" nas propriedades do grupo.
- Certifique-se de que a conta foi adicionada ao grupo de utilizadores.
- Certifique-se de que o nome do grupo de utilizadores registado no equipamento e o nome do grupo no DC (domain controller) são exatamente os mesmos. O DC distingue maiúsculas e minúsculas.
- Certifique-se de que "Usar InfoAut noInícioSessão" foi especificado em "Info. Autent." na conta do utilizador registada no equipamento.
- Se existir mais do que um DC, certifique-se de que foi configurada uma relação confidencial entre cada DC.

W0406-107 : Caso 3

Não é possível resolver o nome do domínio.

- Certifique-se de que é especificado DNS/WINS no nome de domínio em "Definições interface".

W0406-107 : Caso 4

Não é possível estabelecer ligação ao servidor de autenticação.

- Certifique-se de que a ligação ao servidor de autenticação é possível.
- Utilize o "Comando ping" nas "Definições interface" para verificar a ligação.

W0406-107 : Caso 5

Ocorreu um erro com o nome ou a palavra-passe de início de sessão.

- Certifique-se de que o utilizador está registado no servidor.
- Utilize um nome de utilizador e uma palavra-passe de início de sessão.

W0406-107 : Caso 6

Ocorreu um erro de nome de domínio.

- Certifique-se de que o nome de domínio da autenticação Windows está corretamente especificado.

W0406-107 : Caso 7

Não é possível resolver o nome do domínio.

- Especifique o endereço IP no nome de domínio e confirme que a autenticação foi bem sucedida.

  Se a autenticação tiver sido bem sucedida:

  - Se o nome de domínio de nível superior for especificado no nome de domínio (como nomedomínio.xxx.com), certifique-se de que DNS está especificado em "Definições interface".
  - Se um nome de domínio NetBIOS estiver especificado no nome de domínio (como DOMAINNAME), certifique-se de que WINS está especificado em "Definições interface".

  Se a autenticação não tiver sido bem sucedida:

  - Certifique-se de que Restringir LM/NTLM não está definido em "Política de Segurança do Controlador do Domínio" ou "Política de Segurança do Domínio".
  - Certifique-se de que as portas para a firewall de controlo de domínio e a firewall no equipamento para o caminho da ligação de controlo do domínio estão abertas.
- No Windows 7/8/8.1, se a firewall do Windows estiver ativada, crie uma regra de firewall nas "Definições avançadas" da firewall do Windows, para autorizar as portas 137 e 139.
- No Windows XP, se a firewall do Windows estiver ativada, abra a janela das Propriedades para "Ligações de rede" e, em seguida, clique em "Definições" no separador "Avançado". No separador "Excepções", especifique as portas 137 e 139 como excepções.
- Na janela Propriedades para "Ligações de rede", abra as propriedades de TCP/IP. Em seguida, clique nas definições detalhadas, WINS, assinale a caixa "Ativar NetBIOS sobre TCP/IP" e defina o número 137 como "Aberto".

W0406-107 : Caso 8

A autenticação Kerberos falhou.

- As definições da autenticação Kerberos não estão corretamente configuradas.

  Certifique-se de que o nome do realm, o nome KDC (Key Distribution Center) e o nome de domínio sejam devidamente especificados.

- Os tempos do KDC e do equipamento não correspondem.

  A autenticação falhará se a diferença entre o tempo do KDC e o do equipamento for superior a 5 minutos. Certifique-se de que os tempos são coincidentes.

- A autenticação do Kerberos falhará se o nome do realm for especificado em minúsculas. Certifique-se de que o nome do realm é especificado em maiúsculas.

- A autenticação Kerberos falhará se a recuperação automática para o KDC falhar.

  Peça à assistência técnica para certificar-se de que as definições de recuperação do KDC estão definidas para "recuperação automática".

  Se a recuperação automática não estiver a funcionar corretamente, mude para recuperação manual.

W0409-000

Esgotou-se o tempo da autenticação porque o servidor não respondeu.

- Verifique a configuração de rede ou as definições no servidor de autenticação.

W0511-000 / W0517-000

O nome de início de sessão do servidor de autenticação é igual a um nome de utilizador já registado no equipamento. (Os nomes são identificados pelo atributo único especificado nas definições de autenticação do LDAP.)

- Apague o nome antigo duplicado ou mude o nome de início de sessão.
- Se o servidor de autenticação tiver sido alterado recentemente, apague o nome antigo no servidor.

W0606-004

A autenticação falhou porque o nome do utilizador contém palavras que não podem ser utilizadas pelos utilizadores gerais.

- Não utilize "other", "admin", "supervisor" ou "HIDE*" em contas de utilizadores gerais.

W0607-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

W0612-005

A autenticação falhou porque não é possível registar mais utilizadores. (O número de utilizadores registados no livro de endereços atingiu o limite máximo.)

- Peça ao administrador de utilizadores para apagar contas de utilizadores não utilizadas no Livro de Endereços.

W0707-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

W09XX-019

O registo automático do utilizador no servidor falhou durante a autenticação do acesso de um cliente utilizando a função Gestão central do livro de endereços.

- Verifique a ligação de rede entre o cliente e o servidor.
- Não é possível registar utilizadores quando o livro de endereços no servidor está a ser editado.

Autenticação LDAP

L0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador possui sessão iniciada no equipamento e, em seguida, tente novamente.

L0104-000

Não foi possível encriptar uma palavra-passe.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida corretamente.
- [DES] ou [AES] é selecionado para "Chave de encriptação do driver: Grau de encriptação".

  Pode aceder especificando o código de encriptação do driver.
- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está corretamente especificado no driver.

L0206-002

Um utilizador tentou a autenticação a partir de uma aplicação no ecrã "Definições do sistema", onde apenas o administrador tem privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

L0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes carateres proibidos.
- Se o nome da conta foi introduzido incorretamente, introduza-o corretamente e volte a iniciar a sessão.

L0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

L0208-000 / L0208-002

A conta está bloqueada porque o número de tentativas de autenticação permitidas atingiu o limite máximo.

- Peça ao administrador de utilizadores para desbloquear a conta.

L0307-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

L0400-210

Falhou a obtenção de informações de utilizador na procura LDAP.

- Os critérios de busca do atributo de início de sessão podem não ser especificados ou não é possível obter informações de busca especificadas.
- Certifique-se de que o atributo do nome de início de sessão está especificado corretamente.

L0406-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes carateres proibidos.
- Se o nome da conta foi introduzido incorretamente, introduza-o corretamente e volte a iniciar a sessão.

L0406-200

A autenticação não pode ser concluída devido ao número significativo de tentativas de autenticação.

- Aguarde alguns minutos e volte a tentar.
- Se a situação não melhorar, certifique-se de que não está a ocorrer um ataque ao nível da autenticação.
- Notifique o administrador da mensagem do ecrã por e-mail e verifique o registo do sistema quanto a potenciais ataques ao nível da autenticação.

L0406-201

A autenticação está desativada nas definições do servidor LDAP.

- Altere as definições do servidor LDAP nas ferramentas do administrador, em "Definições do sistema".

L0406-202 / L0406-203 : Caso 1

Existe um erro nas definições de autenticação LDAP, no servidor LDAP ou na configuração de rede.

- Certifique-se de que um teste da ligação é bem sucedido com a configuração atual do servidor LDAP.

  Se a ligação não for bem sucedida, é possível que tenha ocorrido um erro nas definições de rede.

  Verifique o nome do domínio ou as definições DNS em "Definições interface".
- Certifique-se de que o servidor LDAP é especificado corretamente nas definições da autenticação LDAP.
- Certifique-se de que o atributo do nome de início de sessão é introduzido corretamente nas definições de autenticação LDAP.
- Certifique-se de que as definições SSL são suportadas pelo servidor LDAP.

L0406-202 / L0406-203 : Caso 2

Ocorreu um erro com o nome de utilizador ou a palavra-passe de início de sessão.

- Certifique-se de que o nome de utilizador e a palavra-passe de início de sessão estão introduzidos corretamente.
- Certifique-se de que um nome de início de sessão utilizável está registado no equipamento.

  A autenticação falhará nos casos seguintes.

  Se o nome de utilizador de início de sessão contiver um espaço, dois pontos (:), ou aspas (").

  Se o nome de utilizador de início de sessão exceder os 128 bytes.

L0406-202 / L0406-203 : Caso 3

Existe um erro no método de encriptação simples.

- A autenticação falhará se a palavra-passe ficar em branco no modo de autenticação simples.

  Para permitir palavras-passe em branco, contacte a assistência técnica.
- No modo de autenticação simples, o DN do nome de utilizador de início de sessão obtém-se na conta do utilizador.

  A autenticação falha se não se conseguir obter o DN.

  Certifique-se de que não existem erros no nome do servidor, no nome de utilizador/palavra-passe de início de sessão ou nas informações introduzidas no filtro de busca.

L0406-204

A autenticação Kerberos falhou.

- As definições da autenticação Kerberos não estão corretamente configuradas.

  Certifique-se de que o nome do realm, o nome do KDC (Key Distribution Center) e o nome do domínio de apoio estão especificados corretamente.

- Os tempos do KDC e do equipamento não correspondem.

  A autenticação falhará se a diferença entre o tempo do KDC e o do equipamento for superior a 5 minutos. Certifique-se de que os tempos são coincidentes.

- A autenticação do Kerberos falhará se o nome do realm for especificado em minúsculas. Certifique-se de que o nome do realm é especificado em maiúsculas.

L0409-000

Esgotou-se o tempo da autenticação porque o servidor não respondeu.

- Contacte o administrador do servidor ou da rede.
- Se a situação não melhorar, contacte a assistência técnica.

L0511-000

O nome de início de sessão do servidor de autenticação é igual a um nome de utilizador já registado no equipamento. (Os nomes são identificados pelo atributo único especificado nas definições de autenticação LDAP.)

- Apague o nome antigo duplicado ou mude o nome de início de sessão.
- Se o servidor de autenticação tiver sido alterado recentemente, apague o nome antigo no servidor.

L0606-004

A autenticação falhou porque o nome do utilizador contém palavras que não podem ser utilizadas pelos utilizadores gerais.

- Não utilize "other", "admin", "supervisor" ou "HIDE*" em contas de utilizadores gerais.

L0607-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

L0612-005

A autenticação falhou porque não é possível registar mais utilizadores. (O número de utilizadores registados no livro de endereços atingiu o limite máximo.)

- Peça ao administrador de utilizadores para apagar contas de utilizadores não utilizadas no Livro de Endereços.

L0707-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e volte a tentar.

L09XX-019

O registo automático do utilizador no servidor falhou durante a autenticação do acesso de um cliente utilizando a função Gestão central do livro de endereços.

- Verifique a ligação de rede entre o cliente e o servidor.
- Não é possível registar utilizadores quando o livro de endereços no servidor está a ser editado.

Se Não For Possível Operar o Equipamento

Se as seguintes condições surgirem enquanto os utilizadores estiverem a utilizar o equipamento, disponibilize instruções sobre como lidar com elas.

Problema	Causa	Solução
Não é possível realizar o seguinte: • Imprimir com o driver de impressão • Ligar com o driver TWAIN	A autenticação de utilizador foi recusada.	Se utilizar a autenticação Windows ou a autenticação LDAP verifique o nome de utilizador e o nome de início de sessão em utilização junto do administrador da rede. Confirme com o administrador de utilizadores se utilizar a autenticação básica.
Não é possível realizar o seguinte: • Imprimir com o driver de impressão • Ligar com o driver TWAIN	O código de encriptação especificado no driver não corresponde ao código de encriptação do driver do equipamento.	Especifique o código de encriptação do driver registado no equipamento. Para obter detalhes, consulte Pág. 151 "Especificar um código de encriptação do controlador".
Não é possível ligar ao driver TWAIN.	A conta, a palavra-passe e o algoritmo de encriptação do SNMPv3 não correspondem às definições especificadas neste equipamento.	Especifique a conta, palavra-passe e o algoritmo de encriptação do SNMPv3 registado no equipamento utilizando as ferramentas de ligação de rede.
Não é possível executar a autenticação utilizando o driver TWAIN.	Outro utilizador tem sessão iniciada no equipamento.	Aguarde que o utilizador encerre a sessão.
Não é possível executar a autenticação utilizando o driver TWAIN.	A autenticação está a demorar devido às condições de funcionamento.	Certifique-se de que a definição do servidor LDAP está correta. Certifique-se de que as definições de rede estão corretas.

Problema	Causa	Solução
Não é possível executar a autenticação utilizando o driver TWAIN.	A autenticação não é possível enquanto o equipamento estiver a editar os dados do livro de endereços.	Aguarde que a edição dos dados do livro de endereços esteja concluída.
Mesmo que introduza o nome de utilizador e a palavra-passe de início de sessão corretos para trabalhar com o livro de endereços no Ridoc IO Device Manager, aparece uma mensagem indicando que foi introduzida uma palavra-passe incorreta.	"Chave encript. driver: Grau de encriptação" não está definido corretamente. Em alternativa, "SSL/TLS" foi ativado embora o certificado necessário não esteja instalado no computador.	Defina "Chave encript. driver: Grau de encriptação" como [Encriptação simples]. Em alternativa, ative "SSL/TLS", instale o certificado do servidor no equipamento e, em seguida, instale o certificado no computador. Para mais informações, consulte Pág. 234 "Especificar as Funções de Segurança Avançadas" e Pág. 112 "Configurar as Definições SSL/TLS".
Não é possível encerrar a sessão utilizando as funções do copiador ou do scanner.	O original não foi completamente digitalizado.	Quando o original tiver sido completamente lido, prima [#], remova o original e, em seguida, encerre a sessão.
"ProgDest" não aparece no ecrã do scanner para especificar destinos.	"Restringir adição de destinos utilizadores" está definido como [Ligado] em "Segurança Avançada", para que apenas o administrador de utilizadores possa registar destinos no livro de endereços no ecrã do scanner.	O registo deve ser efetuado pelo administrador de utilizadores.

Problema	Causa	Solução
Não é possível enviar e-mails a partir do scanner. De igual modo: • Não é possível selecionar um endereço. • Não é possível especificar uma assinatura. • Não é possível guardar dados num suporte.	Seguem-se as causas possíveis: • O período de validade do certificado do utilizador (certificado de destino) expirou. • O período de validade do certificado do dispositivo (S/MIME) expirou. • O certificado do dispositivo (S/MIME) não existe ou é inválido. • Expirou a validade do certificado de dispositivo (PDF com assinatura digital ou PDF/A com assinatura digital). • O certificado de dispositivo (PDF com assinatura digital ou PDF/A com assinatura digital) não existe ou não é válido. • O endereço de e-mail do administrador não é correto.	• Instale um certificado do utilizador (certificado de destino). É possível instalar um certificado do utilizador (certificado de destino) a partir do livro de endereços do Web Image Monitor. O próprio certificado do utilizador (certificado de destino) tem de ser preparado com antecedência. • Instale um certificado do dispositivo para S/MIME. • Instale um certificado de dispositivo para PDF com assinatura digital ou PDF/A com assinatura digital. Para obter detalhes, consulte Pág. 107 "Proteger Vias de Comunicação com um Certificado de Dispositivo". • Especifique o endereço de e-mail do administrador. Para mais informações, consulte Connecting the Machine/ System Settings.

Problema	Causa	Solução
A autenticação do utilizador está desativada; no entanto, os ficheiros guardados não aparecem.	A autenticação do utilizador poderá ter sido desativada sem "Todos os utilizadores" estar selecionado para o acesso do utilizador a ficheiros guardados.	Volte a ativar a autenticação de utilizadores e selecione [Todos os utilizadores] como a definição de permissão de acesso dos ficheiros que pretende visualizar. Para mais informações, consulte Pág. 161 "Gerir Ficheiros Guardados" e a ajuda do Web Image Monitor.
A autenticação do utilizador está desativada, mas os destinos especificados utilizando o equipamento não aparecem.	A autenticação de utilizadores pode ter sido desativada sem que "Todos os utilizadores" fosse selecionado em "Proteger destino".	Volte a ativar a autenticação de utilizadores e, em seguida, selecione [Todos os utilizadores] como a definição da permissão de acesso dos destinos que pretende visualizar. Para obter detalhes, consulte Pág. 73 "Proteger o Livro de Endereços".
Não é possível imprimir quando a autenticação de utilizadores está ativada.	A autenticação de utilizadores pode não ter sido especificada no driver de impressão.	Especifique a autenticação de utilizadores no driver de impressão. Para mais informações, consulte a Ajuda do driver de impressão.
Se tentar interromper um trabalho enquanto copia ou digitaliza, aparece um ecrã de autenticação.	Com este equipamento, pode encerrar a sessão enquanto copia ou digitaliza. Se tentar interromper uma cópia ou uma digitalização após ter encerrado a sessão, aparece um ecrã de autenticação.	Apenas o utilizador que executou um trabalho de cópia ou digitalização pode interromper o mesmo. Aguarde até que o trabalho esteja concluído ou confirme com o utilizador que executou o trabalho. O administrador do equipamento pode eliminar trabalhos.

Problema	Causa	Solução
Após executar "Encriptar defin. personaliz. utiliz.+livro endereços", a mensagem "Sair" não aparece apesar de aguardar durante bastante tempo.	A autenticação pode demorar porque estão registados muitos itens no livro de endereços. Ou, um ficheiro pode estar corrompido ou o disco rígido pode estar avariado.	Se o ecrã ainda não estiver atualizado após decorrer o tempo "Apenas dados sistema fich" especificado em Pág. 77 "Encriptar Dados no Equipamento", contacte a assistência técnica.

9. Lista de Privilégios de Operação para Definições

Este capítulo especifica uma lista dos privilégios de operação para administradores e utilizadores referentes às definições do equipamento quando a autenticação do administrador ou a autenticação do utilizador estiver ativada.

Como Ler

Compreender os cabeçalhos

- Utilizador

  O administrador de utilizadores tem privilégios para esta operação.

- Equip.

  O administrador do equipamento tem privilégios para esta operação.

- Rede

  O administrador de rede tem privilégios para esta operação.

- Fich.

  O administrador de ficheiros tem privilégios para esta operação.

- Remov.

  O utilizador com sessão iniciada tem privilégios para esta operação.

  Em casos em que não estejam selecionadas definições em "Definições disponíveis" de [Gestão de autenticação do administrador].

- Def.

  O utilizador com sessão iniciada tem privilégios para esta operação.

  Estado quando as definições são selecionadas em "Definições disponíveis" de [Gestão de autenticação do administrador].

- Nv.1

  Em casos em que a definição [Menu protegido] está definida como [Nível 1].

- Nv.2

  Em casos em que a definição [Menu protegido] está definida como [Nível 2].

Compreender os símbolos

R/W: É possível executar, alterar e ler.

R: É possível ler.

-: Não é possível executar, alterar, nem ler.

Definições do Sistema

Quando a autenticação de administrador está especificada, as restrições às operações de utilizador variam, dependendo das configurações em "Definições disponíveis".

[Funções gerais]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Programar/Alterar/Apagar texto utiliz.]	R	R/W	R	R	R/W	R
[Tons de teclas do painel]	R	R/W	R	R	R/W	R
[Aviso sonoro de aquecimento]	R	R/W	R	R	R/W	R
[Visor de contagem de cópias]	R	R/W	R	R	R/W	R
[Prioridade de função]	R	R/W	R	R	R/W	R
[Atribuição de tecla de função]	R	R/W	R	R	R/W	R
[Prioridade impressão]	R	R/W	R	R	R/W	R
[Temp reposição função]	R	R/W	R	R	R/W	R
[Saída: impressora]	R	R/W	R	R	R/W	R
[Repetição de tecla]	R	R/W	R	R	R/W	R
[Tempo Visualiz EstadoSist/ListaTrab]	R	R/W	R	R	R/W	R
[Impressão Intercalar]	R	R/W	R	R	R/W	R
[Método p/iniciar alim.]	R	R/W	R	R	R/W	R
[Atraso alim. Original2]	R	R/W	R	R	R/W	R
[Atraso alim. original1]	R	R/W	R	R	R/W	R
[Ajuste fino da escala: Copiador]	R	R/W	R	R	R/W	R
[Ajuste fino da escala: Impressora]	R	R/W	R	R	R/W	R
[Pré-visualizar definições de área]	R	R/W	R	R	R/W	R
[Standard de formato p/papel cortado]*1	R	R/W	R	R	R/W	R
[Prioridade de imagem de impressão]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Teclado externo]	R	R/W	R	R	R/W	R
[ID compatível]	R	R/W	R	R	R/W	R
[Programar/Alterar lista de dispositivos USB]	R	R/W	R	R	R/W	R

*1 Esta definição destina-se aos modelos Região B (principalmente América do Norte).

[Defin. papel band.]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Prioridade bandeja papel: copiador]	R	R/W	R	R	R/W	R
[Prioridade bandeja papel: impressora]	R	R/W	R	R	R/W	R
[Formato do papel da bandeja: Bandeja 1-4]	R	R/W	R	R	R/W	R
[Form. papel alim. manual impressora]	R	R/W	R	R	R/W	R
[Tipo de papel: Alimentação de papel]	R	R/W	R	R	R/W	R
[Tipo de papel: Bandeja 1-4]	R	R/W	R	R	R/W	R
[Espessura do papel: Bandeja de papel]	R	R/W	R	R	R/W	R
[Espessura do papel: Bandeja alim. manual]	R	R/W	R	R	R/W	R
[Volume de papel]	R	R/W	R	R	R/W	R

[Defin. temporiz.]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Temporizador de modo de suspensão]	R	R/W	R	R	R/W	R
[Temporiz. modo de baixo consumo]	R	R/W	R	R	R/W	R
[Temp.reposição automática sistema]	R	R/W	R	R	R/W	R
[Temp. reposição auto copiador/serv doc]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Temporiz. reposição auto impressora]	R	R/W	R	R	R/W	R
[Temp reposição auto scanner]	R	R/W	R	R	R/W	R
[Definir data]	R	R/W	R	R	R/W	R
[Definir tempo]	R	R/W	R	R	R/W	R
[Temp. Encerramento Auto Sessão]	R	R/W	R	R	R/W	R
[Modo desligar fusão (PoupEnerg) Lig/Deslig]	R	R/W	R	R	R/W	R
[Temporizador semanal]	R	R/W	R	R	R/W	R

[Definições interface]

[Rede]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Endereço IPv4 do equipamento]*1	R	R	R/W	R	R/W	R
[Endereço de gateway IPv4]	R	R	R/W	R	R/W	R
[Endereço IPv6 do equipamento]	R	R	R	R	R	R
[Endereço de gateway IPv6]	R	R	R	R	R	R
[Autoconfig. endereço autoconfigurável IPv6]	R	R	R/W	R	R/W	R
[Configuração DHCPv6]	R	R	R/W	R	R/W	R
[Configuração DNS]*2	R	R	R/W	R	R/W	R
[Configuração DDNS]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R
[Nome de Domínio]*1	R	R	R/W	R	R/W	R
[Configuração WINS]	R	R	R/W	R	R/W	R
[Protocolo efetivo]	R	R	R/W	R	R/W	R
[Protocolo de entrega NPC]	R	R	R/W	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[NW Frame Type]	R	R	R/W	R	R/W	R
[Nome computador SMB]	R	R	R/W	R	R/W	R
[Grupo trabalho SMB]	R	R	R/W	R	R/W	R
[Velocidade da Ethernet]	R	R	R/W	R	R/W	R
[Tipo de Rede]	R	R	R/W	R	R/W	R
[Comando ping]	–	–	R/W	–	R/W	R
[Permitir comunicação SNMPv3]	R	R	R/W	R	R/W	R
[Permitir comunicação SSL/ TLS]	R	R	R/W	R	R/W	R
[Nome do Host]	R	R	R/W	R	R/W	R
[Nome do equipamento]	R	R	R/W	R	R/W	R
[Autenticação IEEE 802.1X para Ethernet]	R	R	R/W	R	R/W	R
[Repor predefinições da autenticação IEEE 802.1X]	–	–	R/W	–	R/W	–

*1 Quando a definição para auto-obtenção está ativada, os dados são só de leitura.

*2 Todos os administradores e utilizadores podem executar testes de ligação.

[Wireless LAN]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Modo Comunicação]	R	R	R/W	R	R/W	R
[Definição SSID]	R	R	R/W	R	R/W	R
[Canal Ad-hoc]	R	R	R/W	R	R/W	R
[Método de segurança]	R	R	R/W	R	R/W	R
[Configuração fácil de wireless LAN]	–	–	R/W	–	R/W	–
[Sinal de rede wireless]	R	R	R	R	R	R
[Repor predefinições de fábrica]	–	–	R/W	–	R/W	–

[Imprimir lista]

Definições	Utiliz ador	Equip .	Rede	Fich.	Remo v.	Def.
[Imprimir lista]	–	–	R/W	–	R/W	–

[Transfer. ficheiros]

Definições	Utiliz ador	Equip .	Rede	Fich.	Remo v.	Def.
[Opção de entrega]*3	R	R/W	R	R	R/W	R
[Endereço IPv4 do servidor de captura]	R	R/W	R	R	R/W	R
[Servidor SMTP]	R	R	R/W	R	R/W	R
[Autenticação SMTP]*4	R	R/W	R	R	R/W	R
[POP antes de SMTP]	R	R/W	R	R	R/W	R
[Protocolo de receção]	R	R/W	R	R	R/W	R
[Definições POP3/ IMAP4]	R	R/W	R	R	R/W	R
[Endereço e-mail do admin]	R	R/W	R	R	R/W	R
[Porta de comunicação por e-mail]	R	R	R/W	R	R/W	R
[Intervalo de receção de e-mail]	R	R	R/W	R	R/W	R
[Tamanho máx. de e-mail de receção]	R	R	R/W	R	R/W	R
[Armazenamento e-mail no servidor]	R	R	R/W	R	R/W	R
[Nome de utilizador predefinido/ palavra--passe (envio)]*4	R	R/W	R	R	R/W	R
[Programar/Alterar/Apagar mensagem e--mail]	R	R/W	R	R	R/W	R/W
[Especificar auto nome remetente]	R	R	R/W	R	R/W	R
[Tempo p/reenvio a partir do scanner]	R	R	R/W	R	R/W	R
[Nº reenvios a partir do scanner]	R	R	R/W	R	R/W	R

*3 O equipamento não suporta esta função.

*4 Não é possível ler palavras-passe.

[Ferr. Administrador]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Gestão do livro de endereços]	R/W	R/W *5	R/W *5	R/W *5	R/W*6	R*6
[Livro de Endereços: Programar/Alterar/Apagar Grupo]	R/W	R/W *5	R/W *5	R/W *5	R/W*6	R*6
[Livro de Endereços: Alterar ordem]	R/W	–	–	–	R/W	–
[Imprimir livro de endereços: Lista de destinos]	R/W	–	–	–	R/W	R/W
[Livro de Endereços: Editar Título]	R/W	–	–	–	R/W	–
[Livro de Endereços: Mudar Título]	R/W	–	–	–	R/W	R
[Backup/Recuperação:Defin.personlz.utilz. +livro endereços]	R/W	–	–	–	R/W	–
[Defin transf dados p/programa auto livro endereços]	R/W	R	R	R	R/W	R
[Apagar auto utiliz. livro end.]	R/W	–	–	–	R/W	–
[Apagar todos os dados no livro de endereços]	R/W	–	–	–	R/W	–
[Visualizar/imprimir contador]	R	R/W	R	R	R/W	R/W
[Visualizar/Apagar/Imprimir contador por utilizador]	R/W*7	R/W*8	R	R	R/W	–
[Limitação avançada de volumes de utilização p/ impressão]	R	R/W	R	R	R	R
[Utilização de slot p/dispositivos amovíveis]	R	R/W	R	R	R	R
[Gestão de autenticação de utilizador]	R	R/W	R	R	R/W	R
[Gestão de autenticação otimizada]	R	R/W	R	R	R/W	R
[Gestão de autenticação do administrador]	R/W *9*10	R/W *10	R/W *10	R/W *10	R/W	–

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Programar/ Alterar administrador]	R/W*11	R/W*11	R/W*11	R/W*11	–	–
[Gestão do contador avançado]	R	R/W	R	R	R/W	R
[Gestão da unidade de carregamento externa]	R	R/W	R	R	R/W	R
[Gestão da unidade de carregamento externa avançada]	R	R/W	R	R	R/W	R
[Segurança Avançada]						
• [Código de encriptação do controlador]	–	–	R/W	–	R/W	–
• [Chave encript. driver: Grau de encriptação]	R	R	R/W	R	R/W	R
• [Restringir visualiz. informações utilizador]	R	R/W	R	R	R/W	R
• [Encriptar defin. personaliz. utiliz.+livro endereços]	R/W	R	R	R	R	R
• [Melhorar proteção de ficheiros]	R	R	R	R/W	R	R
• [Restringir utilização de destinos]	R/W	R	R	R	R	R
• [Restringir adição de destinos utilizadores]	R/W	R	R	R	R	R
• [Definições em SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Autenticar trabalho atual]	R	R/W	R	R	R/W	R
• [Política da palavra-passe]	R/W	–	–	–	–	–
• [@Remote Service]	R	R/W	R	R	R/W	R
• [Atualizar firmware]	R	R/W	R	R	–	–
• [Alterar estrutura do firmware]	R	R/W	R	R	–	–
• [Violação da introdução de palavra-passe]	–	R/W	–	–	–	–

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
• [Definição de segurança em caso de violação do acesso]	–	R/W	–	–	–	–
• [Violação do acesso ao dispositivo]	–	R/W	–	–	–	–
[Apagar ficheiro auto no Servidor Doc.]	R	R	R	R/W	R/W	R
[Apagar todos os fich. no Servidor Doc.]	–	–	–	R/W	R/W	–
[Prioridade de captura]	–	R/W	–	–	R/W	R
[Capturar: Apagar fich. não enviados]	–	R/W	–	–	R/W	–
[Captura: Propriedade]	R	R/W	R	R	R/W	R
[Captura: Prioridade pública]	–	R/W	–	–	R/W	R
[Captura: Predefinições proprietário]	–	R/W	–	–	R/W	R
[Programar/Alterar/Apagar servidor LDAP]*4	–	R/W	–	–	R/W	R
[Busca LDAP]	R	R/W	R	R	R/W	R
[Suspensão por temporiz. modo de suspensão]	R	R/W	R	R	R/W	R
[Nível do modo de baixo consumo]	R	R/W	R	R	R/W	R
[Chamada teste de assistência técnica]	–	R/W	–	–	R/W	–
[Notificar sobre o estado do equipamento]	–	R/W	–	–	R/W	–
[Bloquear modo assistência técnica]	R	R/W	R	R	R/W	R
[Versão de firmware]	R	R	R	R	R	R
[Nível de segurança da rede]	R	R	R/W	R	R	R
[Definição Apagar auto memória]	R	R/W	R	R	R	R
[Apagar toda a memória]	–	R/W	–	–	–	–
[Apagar todos os registos]	–	R/W	–	–	R/W	–
[Definição do registo de transferência]*12	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Porta USB fixa]	R	R/W	R	R	R/W	R
[Programar / Alterar / Apagar Realm]	–	R/W	–	–	R/W	R
[Definições de encriptação de dados do equipamento]	–	R/W	–	–	–	–
[Programar/Apagar certificado do dispositivo]	–	–	R/W	–	–	–
[Info.defin.equipamento: Defin. de importação (servidor)]*13	–	–	–	–	–	–
[Info.defin.equipamento: Executar importação (servidor)]*13	–	–	–	–	–	–
[Info. defin. equip.: Exportação (dispositivo de memória)]*13	–	–	–	–	–	–
[Info. defin. equip.: Importação (dispositivo de memória)]*13	–	–	–	–	–	–
[Tipo ficheiro PDF: PDF/A pré-definido]	R	R/W	R	R	R/W	R
[Tecla Parar p/suspender trab. impressão]	R	R/W	R	R	R/W	R
[Tecla de poup. energia p/ mudar modo]	R	R/W	R	R	R/W	R
[Imposição carimbo segurança:Copiador]	R	R/W	R	R	R/W	R
[Imposição carimbo segurança:ServDoc]	R	R/W	R	R	R/W	R
[Imposição de carimbo segurança:Impr.]	R	R/W	R	R	R/W	R
[Personalização do utilizador]	R	R/W	R	R	R/W	R
[Selecionar idiomas disponíveis]	–	R/W	–	–	R/W	–
[Recolher registos]	R	R/W	R	R	R/W	R
[Gestão central do livro de endereços]						
• [Gestão central do livro de endereços]	R	R/W	R	R	R	R
• [Sincronização de clientes]*14	R/W	R/W	R	R	R	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
• [Sincronizar com servidor]*15	R/W	R/W	R	R	R	R

*4 Não é possível ler palavras-passe.

*5 Apenas é possível alterar cabeçalhos e pesquisas de utilizador.

*6 Os itens que podem ser executados, alterados e lidos variam consoante os privilégios de acesso.

*7 Apenas é possível apagar.

*8 Apenas é possível imprimir.

*9 Não é possível alterar quando utilizar a função de autenticação individual.

*10 Apenas é possível alterar as definições dos privilégios de administrador.

*11 Os administradores apenas podem alterar as suas próprias contas.

*12 Apenas é possível alterar para [Desligado].

*13 R/W pode ser executado pelo administrador com todos os privilégios, o que inclui os privilégios de administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros.

*14 É visualizado se utilizar o equipamento como servidor.

*15 É visualizado se utilizar o equipamento como cliente.

Editar Página Principal

Quando a autenticação de administrador está definida, as restrições às operações de utilizador diferem, dependendo das configurações em "Definições disponíveis".

[Editar página principal]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Mover ícone]	R	R/W	R	R	R/W	R
[Apagar ícone]	R	R/W	R	R	R/W	R
[Adicionar ícone]	–	R/W	–	–	R/W	–
[Repor visualiz. ícones predefinida]	–	R/W	–	–	R/W	–
[Inserir imagem no ecrã principal]	–	R/W	–	–	R/W	–

Funções de Copiador/Servidor de Documentos

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

[Funções gerais]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Priorid densid imagem auto]	R	R/W	R	R	R	R
[Priorid. tipo foto original]	R	R/W	R	R	R	R
[Quant. máx. cópias]	R	R/W	R	R	R	R
[Comutação auto bandeja]	R	R/W	R	R	R	R
[Chamada fim trabalho]	R	R/W	R	R	R	R
[Ecrã defin. papel p/alim.man.]	R	R/W	R	R	R	R

[Escala de reprodução]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Escala red/amp utilizador]	R	R/W	R	R	R	R
[Escala de reprodução]	R	R/W	R	R	R	R
[Prioridade escala Red/Amp]	R	R/W	R	R	R	R
[Visualiz. teclas de redução/ampliação]*1	R	R/W	R	R	R	R
[Red/Amp Auto do Utilizador:]	R	R/W	R	R	R	R

*1 Esta definição destina-se aos modelos Região B (principalmente América do Norte).

[Editar]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Ajustar posição]	R	R/W	R	R	R	R
[Apagar largura de bordos]	R	R/W	R	R	R	R

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Apagar sombras no modo Combinar]	R	R/W	R	R	R/W	R
[Linha separação no m. Repet.Imagem]	R	R/W	R	R	R/W	R
[Linha separação no modo Dupla Cópia]	R	R/W	R	R	R/W	R
[Linha de separação no modo Combinar]	R	R/W	R	R	R/W	R
[Ordem de cópia em Combinar]	R	R/W	R	R	R/W	R
[Programar/Apagar formato]	R	R/W	R	R	R/W	R
[Prioridade de Ajuste de margem]	R	R/W	R	R	R	R
[Formato de cópia parcial]	R	R/W	R	R	R	R

[de registo]

[Numeração de fundo]

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Tamanho]	R	R/W	R	R	R/W	R
[Densidade]	R	R/W	R	R	R/W	R

[Carimbo predefin.]

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Idioma do carimbo]	R	R/W	R	R	R/W	R
[Prioridade carimbo]	R	R/W	R	R	R	R
[Formato do carimbo] CÓPIA	R	R/W	R	R	R/W *1	R
[Formato do carimbo] URGENTE	R	R/W	R	R	R/W *1	R
[Formato do carimbo] PRIORIDADE	R	R/W	R	R	R/W *1	R

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Formato do carimbo] Para sua informação.	R	R/W	R	R	R/W *1	R
[Formato do carimbo] PRELIMINAR	R	R/W	R	R	R/W *1	R
[Formato do carimbo] Apenas para uso interno	R	R/W	R	R	R/W *1	R
[Formato do carimbo] CONFIDENCIAL	R	R/W	R	R	R/W *1	R
[Formato do carimbo] RASCUNHO	R	R/W	R	R	R/W *1	R

*1 Apenas é possível especificar ajustes à posição de impressão. Não é possível configurar a própria posição de impressão.

[Carimbo utiliz.]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Programar/Eliminar carimbo]	R	R/W	R	R	R/W	R
[Formato do carimbo] 1-40	R	R/W	R	R	R/W	R

[Carimbo da data]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Formato]	R	R/W	R	R	R	R
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R
[Sobrepor]	R	R/W	R	R	R/W	R
[Definição carimbo]	R	R/W	R	R	R/W *2	R

*2 Apenas é possível definir ajustes da posição de impressão. Não é possível configurar a própria posição de impressão.

[Numeração página]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Formato do carimbo]	R	R/W	R	R	R	R
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R
[Numeração de páginas em Combinar]	R	R/W	R	R	R/W	R
[Posição do carimbo:P1,P2...]	R	R/W	R	R	R/W *3	R
[Posição do carimbo:1/5,2/5..]	R	R/W	R	R	R/W *3	R
[Posição do carimbo:-1-,-2-...]	R	R/W	R	R	R/W *3	R
[Posição do carimbo:P.1,P.2...]	R	R/W	R	R	R/W *3	R
[Posição do carimbo:1,2...]	R	R/W	R	R	R/W *3	R
[Posição do carimbo:1-1,1-2...]	R	R/W	R	R	R/W *3	R
[Sobrepor]	R	R/W	R	R	R/W	R
[Letra inicial da numeração de página]	R	R/W	R	R	R	R

*3 Apenas é possível definir ajustes à posição de impressão. Não é possível configurar a própria posição de impressão.

[Texto do carimbo]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R
[Sobrepor]	R	R/W	R	R	R/W	R
[Definição carimbo]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Alterar n.º série trab. p/ 1.º trabalho]	R	R/W	R	R	R	R

[Entrada/Saída]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Coleção eletrón.: Cont.Auto Papel]	R	R/W	R	R	R	R

[Ferr. Administrador]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Menu protegido]	R	R/W	R	R	R	R

Funções da Impressora

Esta secção lista as funções da impressora que aparecem se premir [Impressora] no Página principal.

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

Funções da Impressora

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Lista de trabalhos]	R	R	R	R	R	R
[Trabalhos de impressão]	R	R	R	R/W	R/W	R/W
[Imprimir de dispositivo de memória]	–	–	–	–	R/W	R/W
[Apagar trabalho]	R/W	R/W	R/W	R/W	R/W	R/W
[Detalhes dos trabalhos]	R/W	R/W	R/W	R/W	R/W	R/W
[Avanço de página]	R/W	R/W	R/W	R/W	R/W	R/W
[Lista trab. em spool]	R	R/W	R	R	R	R
[Registo de erro]	–	R	–	–	R	R

Funções de Impressora

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

[Impr. Lista/ Teste]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Listas múltiplas]	–	R/W	–	–	R/W	R/W
[Página de configuração]	–	R/W	–	–	R/W	R/W
[Registo de erro]	–	R/W	–	–	R/W	R/W
[Página de configuração PS/ fontes]	–	R/W	–	–	R/W	R/W
[Página de configuração PDF/ fontes]	–	R/W	–	–	R/W	R/W
[Lista de definições impressão (RTIFF)]	–	R/W	–	–	R/W	R/W
[Lista de definições impressão (RPGL)]	–	R/W	–	–	R/W	R/W
[Hex Dump]	–	R/W	–	–	R/W	R/W

[Gestão de dados]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Menu protegido]	R	R/W	R	R	R	R
[Bloquear impressão lista/teste]	R	R/W	R	R	R	R
[Apag. todos trab. impr. temporários]	–	–	–	R/W	–	–
[Apagar todos trab. impr. guardada]	–	–	–	R/W	–	–
[Apag. auto trab. impr. temporários]	R	R	R	R/W	R	R
[Apag. auto fich. impressão guardada]	R	R	R	R/W	R	R

[Sistema]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Relatório de erros de impressão]	R	R/W	R	R	R	R
[Continuar auto]	R	R/W	R	R	R	R
[Guardar e não imprimir trabalho c/erro]	R	R/W	R	R	R	R
[Sobrecarga da memória]	R	R/W	R	R	R	R
[Coleção eletrón.: Cont.Auto Papel]	R	R/W	R	R	R	R
[Rodar 180 graus]	R	R/W	R	R	R	R
[Imprimir dados compactados]	R	R/W	R/W	R	R	R
[Utilização da memória]	R	R/W	R	R	R	R
[Cópias]	R	R/W	R	R	R	R
[Impressão de página em branco]	R	R/W	R	R	R	R
[Poupança de toner]	R	R/W	R	R	R	R
[Tempo espera trab reservado]	R	R/W	R	R	R	R
[Linguagem da Impressora]	R	R/W	R	R	R	R
[Formato secundário]	R	R/W	R	R	R	R
[Prioridade de definição de bandeja]	R	R/W	R	R	R	R
[Impressão Margem a Margem]	R	R/W	R	R	R	R
[Predefinição da linguagem da impressora]	R	R/W	R	R	R	R
[Comutação de bandeja]	R	R/W	R	R	R	R
[Comut. auto avanç. bandeja]	R	R/W	R	R	R	R
[Trabs. não impressos pq. equip.desligado]	R	R/W	R	R	R	R
[Mudar ecrã inicial]	R	R/W	R	R	R	R

[Sistema(EM)]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Impressão de página em branco]	R	R/W	R	R	R	R
[Limite tempo para alimentação]	R	R/W	R	R	R	R
[Form personaliz: Bandeja 1-4]	R	R/W	R	R	R	R

[Controladora]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Memória E/S]	R	R/W	R	R	R	R
[Limite de tempo E/S]	R	R/W	R	R	R	R

[Menu PostScript]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

[Menu PDF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

[Menu RTIFF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

[Menu RPGL]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

Funções de Scanner

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

[Definições Gerais]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Mudar título]	R	R/W	R	R	R	R
[Procurar destino]	R	R/W	R	R	R	R
[Autentic. externa: Defin. subst. caminho]	R	R/W	R	R	R	R
[Tempo de espera TWAIN]	R	R/W	R	R	R	R
[Prioridade visor da lista destinos 1]*1	R	R/W	R	R	R	R
[Prioridade visor da lista destinos 2]	R	R/W	R	R	R	R
[Imprimir e apagar jornal do scanner]	R	R/W	R	R	R	R
[Imprimir jornal do scanner]	R	R/W	R	R	R	R
[Apagar jornal do scanner]	R	R/W	R	R	R	R
[Apagar destinos recentes]	R	R/W	R	R	R	R
[Definição programada para destinos]	R	R/W	R	R	R	R

*1 O equipamento não suporta esta função.

[Definições digitalização]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Defin tempo p/ origin seg]	R	R/W	R	R	R	R
[Densidade de fundo de ADS (Cor integral)]	R	R/W	R	R	R	R
[Saída de originais (TWAIN)]	R	R/W	R	R	R	R
[Escala de reprodução]	R	R/W	R	R	R	R
[Visualiz. teclas de redução/ampliação]*1	R	R/W	R	R	R	R

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Program./Alt./Apag. form. digitaliz.]	R	R/W	R	R	R	R

*1 Esta definição destina-se aos modelos Região B (principalmente América do Norte).

[Definições de envio]

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Compactação (Preto e Branco)]	R	R/W	R	R	R/W	R
[Método de compactação (P&B)]	R	R/W	R	R	R/W	R
[Compactação(Escala cinzentos/Cor integral)]	R	R/W	R	R	R/W	R
[PDF nível elevado de compactação (JPEG 2000)]	R	R/W	R	R	R/W	R
[PDF lido c/ OCR: Deteção pág. em branco]	R	R/W	R	R	R/W	R
[Tamanho máx. de e-mail]	R	R	R/W	R	R	R
[Dividir e enviar e-mail]	R	R	R/W	R	R	R
[Inserir informações de e-mail adicionais]	R	R/W	R	R	R/W	R
[Nº dígitos p/ficheiros página única]	R	R/W	R	R	R/W	R
[Método envio p/e-mail de fich.guardado]	R	R/W	R	R	R/W	R
[Endereço de e-mail predefinido]	R	R/W	R	R	R	R

[Definições Iniciais]

Definições	Utiliz ador	Equip .	Rede	Fich.	Nv.1	Nv.2
[Menu protegido]	R	R/W	R	R	R	R

Funções de Browser

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Predefinições de browser]	R	R/W	R	R	R/W	R
[Definições por utilizadores]	R	R/W	R	R	R/W	R
[Visualizar registos]	R	R	R	R	R	R

Definições de Função Avançada

[Defin. de função avançada]

Definições	Utiliz ador	Equip .	Rede	Fich.	Remo v.	Def.
[Definição Arranque]	R	R/W	R	R	R	R
[Instalar]	R	R/W	R	R	R	R
[Desinstalar]	R	R/W	R	R	R	R
[Info Função Avançada]	R	R/W	R	R	R	R
[Ferr. Administrador]	–	R/W	–	–	–	–
[Defin de arranque de progr adicional]	R	R/W	R	R	R	R
[Instalar progr adicional]	R	R/W	R	R	R	R
[Desinstalar progr adic]	R	R/W	R	R	R	R
[Informações progr adicional]	R	R/W	R	R	R	R

Web Image Monitor: Trabalho

Estas definições estão em [Estado/Informações].

Os utilizadores apenas podem alterar os trabalhos que tenham sido eles próprios a executar.

[Lista de trabalhos]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Trabalhos atuais/em espera]: [Apagar reserva]	–	R/W	–	–	–	R/W
[Trabalhos atuais/em espera]: [Suspender impressão]/[Retomar impressão]	–	R/W	–	–	–	–
[Trabalhos atuais/em espera]: [Alterar ordem]	–	R/W	–	–	–	–
[Histórico de trabalhos]	–	R	–	–	R	R*1

*1 Pode ser visualizado se a autenticação de código de utilizador for ativada para o método de autenticação de utilizador.

[Impressora]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Impressão em spool]: [Apagar]	R	R/W	R	R	R	R
[Histórico de trabalhos]	R	R/W	R	R	R	R
[Registo de erros]	–	R	–	–	R	R
[Web Printing Tool]	R/W	R/W	R/W	R/W	R/W	R/W

[Servidor de documentos]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Histórico de trabalhos de impressão]	–	R	–	–	R	R*1
[Histórico de envios remotos do scanner]	–	R	–	–	R	R*1

*1 Pode ser visualizado se a autenticação de código de utilizador for ativada para o método de autenticação de utilizador.

Web Image Monitor: Definições do dispositivo

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

[Sistema]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Nome do dispositivo]	R	R	R/W	R	R/W	R
[Observação]	R	R	R/W	R	R/W	R
[Localização]	R	R	R/W	R	R/W	R
[Idioma do painel]	R	R/W	R	R	R/W	R
[Impressão em spool]	R	R/W	R	R	R/W	R
[Proteger painel do visor de impressora]	R	R/W	R	R	–	–
[Prioridade de impressão]	R	R/W	R	R	R/W	R
[Temporizador de reposição de função]	R	R/W	R	R	R/W	R
[Tecla de poupança de energia para mudar de modo]	R	R/W	R	R	R/W	R
[Tecla Parar para suspender trabalho de impressão]	R	R/W	R	R	R/W	R
[Visualizar endereço IP no painel do visor do dispositivo]	R	R/W	R	R	–	–
[Utilização de slot para dispositivos amovíveis]	R	R/W	R	R	R	R
[ID compatível]	R	R/W	R	R	R/W	R
[Tipo de ficheiro PDF: PDF/A pré-definido]	R	R/W	R	R	R/W	R
[Proibir imprimir ficheiros guardados do Web Image Monitor]	R	R/W	R	R	R	R
[Bandeja de saída]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Prioridade de bandeja de papel]	R	R/W	R	R	R/W	R

[Atribuição de tecla de função/Prioridade de função]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Atribuição de tecla de função]	R	R/W	R	R	R/W	R
[Prioridade de função]	R	R/W	R	R	R/W	R

[Papel]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Bandeja 1-4]	R	R/W	R	R	R/W	R
[Alimentação manual de papel]	R	R/W	R	R	R/W	R
[Deteção de pouco papel]	R	R/W	R	R	R	R

[Data/Hora]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Definir data]	R	R/W	R	R	R/W	R
[Definir hora]	R	R/W	R	R	R/W	R
[Nome do servidor SNTP]	R	R/W	R	R	R/W	R
[Intervalo de polling SNTP]	R	R/W	R	R	R/W	R
[Fuso horário]	R	R/W	R	R	R/W	R

[Temporizador]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Temporizador de modo de suspensão]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Temporizador de modo de baixo consumo]	R	R/W	R	R	R/W	R
[Temporizador de reposição automática do sistema]	R	R/W	R	R	R/W	R
[Temporizador de reposição automática do copiador/servidor de documentos]	R	R/W	R	R	R/W	R
[Temporizador de reposição automática do scanner]	R	R/W	R	R	R/W	R
[Temporizador de reposição automática da impressora]	R	R/W	R	R	R/W	R
[Temporizador para encerramento automático da sessão]	R	R/W	R	R	R/W	R
[Modo de desligar fusão Ligar/Desligar]	R	R/W	R	R	R/W	R
[Temporizador semanal]	R	R/W	R	R	R/W	R

[Registos]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Registo de trabalhos]	R	R/W	R	R	R/W	R
[Registo de acessos]	R	R/W	R	R	R/W	R
[Registos ecológicos]	R	R/W	R	R	R/W	R
[Transferir registos]*2	R	R/W	R	R	R/W	R
[Código de classificação]	R	R/W	R	R	R/W	R
[Apagar todos os registos]	–	R/W	–	–	R/W	–

*2 Apenas é possível alterar para [Inativo].

[Download de registos]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Registos para download]	–	R/W	–	–	–	–
[Download]	–	R/W	–	–	–	–

[E-mail]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Endereço de e-mail do administrador]	–	R/W	–	–	R/W	R
[Especificar auto nome remetente]	–	R/W	–	–	R/W	R
[Assinatura]	–	R/W	–	–	R/W	R
[Protocolo de receção]	–	R/W	–	–	R/W	R
[Intervalo de receção de e-mail]	–	–	R/W	–	R/W	R
[Tamanho máximo de e-mail a receber]	–	–	R/W	–	R/W	R
[Armazenamento de e-mail no servidor]	–	–	R/W	–	R/W	R
[Nome do servidor SMTP]	–	–	R/W	–	R/W	R
[N.º porta SMTP]	–	–	R/W	–	R/W	R
[Utilizar ligação segura (SSL)]	–	–	R/W	–	R/W	R
[Autenticação SMTP]	–	R/W	–	–	R/W	R
[Endereço de e-mail de autenticação SMTP]	–	R/W	–	–	R/W	R
[Nome do utilizador de autenticação SMTP]	–	R/W	–	–	R/W	–
[Palavra-passe de autenticação SMTP]*3	–	R/W	–	–	R/W	–
[Encriptação de autenticação SMTP]	–	R/W	–	–	R/W	R
[POP antes de SMTP]	–	R/W	–	–	R/W	R
[Endereço de e-mail POP]	–	R/W	–	–	R/W	R
[Nome de utilizador POP]	–	R/W	–	–	R/W	–

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Palavra-passe POP]*3	–	R/W	–	–	R/W	–
[Definição de limite de tempo após autenticação POP]	–	R/W	–	–	R/W	R
[Nome do servidor POP3/IMAP4]	–	R/W	–	–	R/W	R
[Encriptação POP3/IMAP4]	–	R/W	–	–	R/W	R
[N.º de porta de receção POP3]	–	–	R/W	–	R/W	R
[N.º de porta de receção IMAP4]	–	–	R/W	–	R/W	R
[Endereço de e-mail para notificação por e--mail]	–	R/W	–	–	R/W	R
[Receber notificação por e-mail]	–	R/W	–	–	R/W	–
[Nome de utilizador para notificação por e--mail]	–	R/W	–	–	R/W	–
[Palavra-passe para notificação por e--mail]*3	–	R/W	–	–	R/W	–

*3 Não é possível ler palavras-passe.

[Notificação automática por e-mail]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Mensagem de notificação]	R	R/W	R	R	R/W	R
[Grupos a notificar]	R	R/W	R	R	R/W	R
[Selecionar grupos/itens a notificar]	R	R/W	R	R	R/W	R
[Definições detalhadas de cada item]	R	R/W	R	R	R/W	R

[Notificação por e-mail a pedido]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Assunto da notificação]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Mensagem de notificação]	R	R/W	R	R	R/W	R
[Restrição de acesso a informações]	R	R/W	R	R	R/W	R
[Endereço de e-mail a receber/Definições do nome de domínio]	R	R/W	R	R	R/W	R

[Transferência de ficheiros]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Nome de utilizador SMB]	–	R/W	–	–	R/W	–
[Palavra-passe SMB]*3	–	R/W	–	–	R/W	–
[Nome de utilizador FTP]	–	R/W	–	–	R/W	–
[Palavra-passe FTP]*3	–	R/W	–	–	R/W	–
[Nome do utilizador NPC]	–	R/W	–	–	R/W	–
[Palavra-passe NCP]*3	–	R/W	–	–	R/W	–

*3 Não é possível ler palavras-passe.

[Gestão da autenticação de utilizador]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Gestão da autenticação de utilizador]	R	R/W	R	R	R/W	R
[Definições de autenticação dos trabalhos da impressora]	R	R/W	R	R	R/W	R
[Definições de autenticação por código de utilizador]	R	R/W	R	R	R/W	R
[Definições de autenticação básica]	R	R/W	R	R	R/W	R
[Definições de autenticação Windows]	R	R/W	R	R	R/W	R
[Definições de grupo para autenticação Windows]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Definições de autenticação LDAP]	R	R/W	R	R	R/W	R

[Gestão de autenticação do administrador]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Autenticação do administrador de utilizadores]	R/W	R	R	R	R	R
[Autenticação do administrador do equipamento]	R	R/W	R	R	R	R
[Autenticação do administrador de rede]	R	R	R/W	R	R	R
[Autenticação do administrador de ficheiros]	R	R	R	R/W	R	R

[Programar/Alterar administrador]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Administrador de utilizadores]	R/W	R	R	R	–	–
[Administrador do equipamento]	R	R/W	R	R	–	–
[Administrador da rede]	R	R	R/W	R	–	–
[Administrador de ficheiros]	R	R	R	R/W	–	–
[Nome de utilizador de início de sessão]*4	R/W	R/W	R/W	R/W	–	–
[Palavra-passe de início de sessão]*4	R/W	R/W	R/W	R/W	–	–
[Palavra-passe da encriptação]*4	R/W	R/W	R/W	R/W	–	–

*4 Os administradores apenas podem alterar as suas próprias contas.

[Servidor LDAP]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Busca LDAP]	–	R/W	–	–	R/W	–

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Alterar]	–	R/W	–	–	R/W	–
[Apagar]	–	R/W	–	–	R/W	–

[Atualização do firmware]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Atualizar]	–	R/W	–	–	–	–
[Versão do firmware]	–	R	–	–	–	–

[Autenticação Kerberos]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Algoritmo de encriptação]	–	R/W	–	–	–	–
[Realm 1-5]	–	R/W	–	–	–	–

[Informações de definição do equipamento: Definição de importação (servidor)]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Importar ficheiro a partir de]*5	–	–	–	–	–	–
[Importação programada a hora especificada]*5	–	–	–	–	–	–
[Comparar novo ficheiro com o último ficheiro de importação]*5	–	–	–	–	–	–
[Notificação de falha por e-mail]*5	–	–	–	–	–	–
[Número de tentativas]*5	–	–	–	–	–	–
[Intervalo para voltar a tentar]*5	–	–	–	–	–	–
[Chave de encriptação]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, o que inclui os privilégios de administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros.

[Teste de importação]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Iniciar]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, o que inclui os privilégios de administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros.

[Importar/Exportar informações de definição do equipamento]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Exportar informações de definição do equipamento]*5	–	–	–	–	–	–
[Importar informações de definição do equipamento]*5	–	–	–	–	–	–
[Exportar ficheiro de imagem para ecrã inicial]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, o que inclui os privilégios de administrador de utilizadores, administrador do equipamento, administrador de rede e administrador de ficheiros.

[Imposição de carimbo de segurança]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Copiador]	R	R/W	R	R	R	R
[Servidor de documentos]	R	R/W	R	R	R	R
[Impressora]	R	R/W	R	R	R	R

[Programar/Alterar lista de dispositivos USB]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Dispositivo 1]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Dispositivo 2]	R	R/W	R	R	R/W	R

Web Image Monitor: Impressora

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

[Definições básicas]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Relatório de erros de impressão]	R	R/W	R	R	R	R
[Continuar automaticamente]	R	R/W	R	R	R	R
[Sobrecarga da memória]	R	R/W	R	R	R	R
[Coleção eletrónica: Continuação automática de papel]	R	R/W	R	R	R	R
[Apagar automaticamente trabalhos de impressão temporários]	R	R	R	R/W	R	R
[Apagar automaticamente trabalhos de impressão guardados]	R	R	R	R/W	R	R
[Trabalhos por imprimir enquanto o equipamento esteve desligado]	R	R/W	R	R	R	R
[Rodar 180 graus]	R	R/W	R	R	R	R
[Imprimir dados compactados]	R	R/W	R/W	R	R	R
[Uso da memória]	R	R/W	R	R	R	R
[Cópias]	R	R/W	R	R	R	R
[Impressão de página em branco]	R	R/W	R	R	R	R
[Poupança de toner]	R	R/W	R	R	R	R
[Tempo de espera do trabalho reservado]	R	R/W	R	R	R	R
[Linguagem da impressora]	R	R/W	R	R	R	R
[Formato de papel secundário]	R	R/W	R	R	R	R
[Prioridade de definição de bandeja]	R	R/W	R	R	R	R

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Guardar e não imprimir trabalho com erro]	R	R/W	R	R	R	R
[Impressão de margem a margem]	R	R/W	R	R	R	R
[Linguagem de impressora predefinida]	R	R/W	R	R	R	R
[Comutação de bandeja]	R	R/W	R	R	R	R
[Bloqueio da função de impressão de listas/ teste]	R	R/W	R	R	R	R
[Comutação automática avançada de bandeja]	R	R/W	R	R	R	R
[Definição de mudança do ecrã inicial]	R	R/W	R	R	R	R
[Controladora]	R	R/W	R	R	R	R
[Menu PS]	R	R/W	R	R	R	R
[Menu PDF]	R	R/W	R	R	R	R

[Parâmetros de bandeja (PS)]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Parâmetros de bandeja (PS)]	–	R/W	–	–	–	–

[Palavra-passe temporária de PDF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Palavra-passe temporária de PDF]	–	–	–	–	R/W	R/W

[Palavra-passe para grupo PDF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Palavra-passe para grupo PDF]	–	R/W	–	–	–	–

[Palavra-passe fixa de PDF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Palavra-passe fixa de PDF]	–	R/W	–	–	–	–

[Menu RTIFF]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

[Menu RPGL]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
Todas as definições	R	R/W	R	R	R	R

[Permissões para a linguagem da impressora aceder ao sistema de ficheiros]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[PJL]	R	R/W	R	R	R	R
[RPDL]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: Scanner

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam consoante a definição em "Menu protegido".

[Definições gerais]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Mudar título]	R	R/W	R	R	R	R
[Procurar destino]	R	R/W	R	R	R	R
[Tempo de espera para comando de digitalização a partir do PC]	R	R/W	R	R	R	R
[Prioridade de visualização 2 da lista de destinos]	R	R/W	R	R	R	R
[Imprimir e apagar jornal do scanner]	R	R/W	R	R	R	R
[Autenticação externa: Definição de substituição do caminho]	R	R/W	R	R	R	R

[Definições de leitura]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Tempo de espera para originais seguintes]	R	R/W	R	R	R	R
[Densidade de fundo para ADS (Cor integral)]	R	R/W	R	R	R	R

[Definições de envio]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Compactação (Preto e branco)]	R	R/W	R	R	R/W	R
[Compactação (Escala de cinzentos/Cor integral)]	R	R/W	R	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[PDF lido com OCR: Detecção de página em branco]	R	R/W	R	R	R/W	R
[PDF nível elevado de compactação (JPEG 2000)]	R	R/W	R	R	R/W	R
[Tamanho máximo de e-mail]	R	R	R/W	R	R*1	R*1
[Dividir e enviar e-mail]	R	R	R/W	R	R*1	R*1
[Introduzir informações de e-mail adicionais]	R	R/W	R	R	R/W	R
[N.º de dígitos para ficheiros de uma página]	R	R/W	R	R	R/W	R
[Stored File Email Method]	R	R/W	R	R	R/W	R
[Assunto de e-mail predefinido]	R	R/W	R	R	R	R

*1 Quando [Gestão de rede] em [Gestão de autenticação do administrador] está definido como [Desligado], os utilizadores recebem os privilégios R/W.

[Definições iniciais]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Menu protegido]	R	R/W	R	R	R	R

[Predefinições de ecrãs normais no dispositivo]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Guardar ficheiro]	–	R/W	–	–	R	R
[Pré-visualizar]	–	R/W	–	–	R	R
[Definições de leitura]	–	R/W	–	–	R	R
[Tipo de ficheiro de envio]	–	R/W	–	–	R	R

[Predefinições de ecrãs simplificados no dispositivo]

Definições	Utilizador	Equip.	Rede	Fich.	Nv.1	Nv.2
[Definições de leitura]	–	R/W	–	–	R	R
[Tipo de ficheiro de envio]	–	R/W	–	–	R	R

Web Image Monitor: Interface

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

[Definições do interface]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Tipo de rede]	–	–	R/W	–	R	–
[Rede]	R	R	R	R	R	R
[Endereço MAC]	R	R	R	R	R	R
[Segurança Ethernet]	R	R	R/W	R	R/W	R
[Velocidade Ethernet]	R	R	R/W	R	R/W	R
[USB]	R	R/W	R	R	R/W	R
[Controladora USB]	R	R/W	R	R	R/W	R

[Definições de wireless LAN]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Tipo de rede]	–	–	R/W	–	R	–
[Rede]	R	R	R	R	R	R
[Endereço MAC]	R	R	R	R	R	R
[Wireless LAN disponível]	R	R	R	R	R	R
[Modo de comunicação]	R	R	R/W	R	R/W	R
[SSID]	R	R	R/W	R	R/W	R
[Canal]	R	R	R/W	R	R/W	–
[Método de segurança]	R	R	R/W	R	R/W	R
[Definições WEP]	R	R	R/W	R	R/W	R

Definições	Utiliz ador	Equip .	Rede	Fich.	Remo v.	Def.
[Definições WPA2]	R	R	R/W	R	R/W	R

Web Image Monitor: Rede

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

[IPv4]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[IPv4]	R	R	R/W *1	R	R/W *1	R
[Nome do host]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Nome de domínio]	R	R	R/W	R	R/W	R
[Endereço IPv4]	R	R	R/W	R	R/W	R
[Máscara de subrede]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Servidor WINS principal]	R	R	R/W	R	R/W	R
[Servidor WINS secundário]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Intervalo de ID]	R	R	R/W	R	R/W	R
[Detalhes]	R	R	R/W	R	R/W	R

*1 Não é possível desativar o IPv4 se utilizar o Web Image Monitor através de uma ligação IPv4.

[IPv6]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[IPv6]	R	R	R/W *2	R	R/W *2	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Nome do host]	R	R	R/W	R	R/W	R
[Nome de domínio]	R	R	R/W	R	R/W	R
[Endereço link-local]	R	R	R	R	R	R
[Endereço Autoconfigurável]	R	R	R/W	R	R/W	R
[Endereço de configuração manual]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[Endereço DHCPv6]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Detalhes]	R	R	R/W	R	R/W	R

*2 Não é possível desativar o IPv6 se utilizar o Web Image Monitor através de uma ligação IPv6.

[NetWare]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[NetWare]	R	R	R/W	R	R/W	R
[Definições de impressão NetWare]	R	R	R/W	R	R/W	R
[Entrega NPC]	R	R	R/W	R	R/W	R

[SMB]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[SMB]	R	R	R/W	R	R/W	R
[Protocolo]	R	R	R	R	R	R
[Nome do grupo de trabalho]	R	R	R/W	R	R/W	R
[Nome do computador]	R	R	R/W	R	R/W	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Observação]	R	R	R/W	R	R/W	R
[Nome de partilha]	R	R	R	R	R	R
[Notificar fim de impressão]	R	R	R/W	R	R/W	R

[SNMP]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[SNMP]	–	–	R/W	–	–	–
[Protocolo]	–	–	R/W	–	–	–
[Definição SNMPv1,v2]	–	–	R/W	–	–	–
[Comunidade]	–	–	R/W	–	–	–

[SNMPv3]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[SNMP]	–	–	R/W	–	–	–
[Protocolo]	–	–	R/W	–	–	–
[Definição SNMPv3]	–	–	R/W	–	–	–
[Definição da comunicação TRAP SNMPv3]	–	–	R/W	–	–	–
[Conta (Utilizador)]	–	–	R/W	–	–	–
[Conta (Administrador de rede)]	–	–	R/W	–	–	–
[Conta (Administrador de equipamento)]	–	R/W	–	–	–	–

[SSDP]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[SSDP]	–	–	R/W	–	–	–

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[UUID]	–	–	R	–	–	–
[Validade do perfil]	–	–	R/W	–	–	–
[TTL]	–	–	R/W	–	–	–

[Bonjour]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Bonjour]	R	R	R/W	R	R/W	R
[Nome do host local]	R	R	R	R	R	R
[Detalhes]	R	R	R/W	R	R/W	R
[Prioridade de ordem de impressão]	R	R	R/W	R	R/W	R

[Registo do sistema]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Registo do sistema]	R	R	R	R	R	–

Web Image Monitor: Segurança

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Segurança da rede]	–	–	R/W	–	–	–
[Controlo de acesso]	–	–	R/W	–	–	–
[Autenticação IPP]	–	–	R/W	–	–	–
[SSL/TLS]	–	–	R/W	–	–	–
[ssh]	–	–	R/W	–	R	R
[Certificado externo]	–	–	R/W	–	–	–
[Certificado do dispositivo]	–	–	R/W	–	–	–
[S/MIME]	–	–	R/W	–	–	–
[IPsec]	–	–	R/W	–	–	–
[Política de bloqueio de utilizador]	–	R/W	–	–	–	–
[IEEE 802.1X]	–	–	R/W	–	–	–
[Segurança Avançada]						
• [Chave de encriptação do driver]	–	–	R/W	–	R/W	–
• [Chave de encriptação do driver: Grau de encriptação]	R	R	R/W	R	R/W	R
• [Restringir visualização de informações de utilizador]	R	R/W	R	R	R/W	R
• [Encriptar definições personalizadas de utilizador e livro de endereços]	R/W	R	R	R	R	R
• [Aumentar proteção de ficheiros]	R	R	R	R/W	R	R
• [Restringir utilização de destinos (scanner)]	R/W	R	R	R	R	R
• [Restringir adição de destinos de utilizador (scanner)]	R/W	R	R	R	R	R

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
• [Autenticar trabalho atual]	R	R/W	R	R	R/W	R
• [Serviço @Remote]	R	R/W	R	R	R/W	R
• [Atualizar firmware]	R	R/W	R	R	–	–
• [Alterar estrutura do firmware]	R	R/W	R	R	–	–
• [Política de palavra-passe]	R/W	–	–	–	–	–
• [Definições por SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Definição de segurança em caso de violação de acesso]	–	R/W	–	–	–	–
• [Password Entry Violation]	–	R/W	–	–	–	–
• [Violação do acesso ao dispositivo]	–	R/W	–	–	–	–

Web Image Monitor: @Remote

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Configurar RC Gate]	–	R/W	–	–	–	–
[Atualizar firmware do RC Gate]	–	R/W	–	–	–	–
[Servidor proxy do RC Gate]	–	R/W	–	–	–	–
[Notificar problemas funcionais do equipamento]	–	R/W	–	–	–	–

Web Image Monitor: Página web

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

[Página web]

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Idioma da página web]	R	R	R/W	R	R/W	R
[Encerrar sessão do Web Image Monitor automaticamente]	R	R	R/W	R	R/W	R
[Definir endereço de URL da página de link]	R	R	R/W	R	R/W	R
[Definir endereço de URL da Ajuda]	R	R	R/W	R	R/W	R
[WSD/Definição UPnP]	R	R	R/W	R	R/W	R
[Download de ficheiro de ajuda]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: Definições de função avançada

Estas definições pertencem à [Configuração] em [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Definição da instalação]	–	R/W	–	–	–	–
[Informações de função avançada]	R	R	R	R	R	R
[Instalar]	–	R/W	–	–	–	–
[Desinstalar]	–	R/W	–	–	–	–
[Ferramentas do administrador]	–	R/W	–	–	–	–
[Definição de arranque de programa adicional]	–	R/W	–	–	–	–
[Instalar programa adicional]	–	R/W	–	–	–	–
[Desinstalar programa adicional]	–	R/W	–	–	–	–
[Copiar funções avançadas]	–	R/W	–	–	–	–
[Copiar dados de guardar no cartão]	–	R/W	–	–	–	–

Web Image Monitor: Livro de endereços

Estas definições pertencem a [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Adicionar utilizador]	R/W	–	–	–	R/W*1	R/W*1
[Alterar]	R/W	–	–	–	R/W*1	R/W*1
[Apagar]	R/W	–	–	–	R/W*1	R/W*1
[Adicionar grupo]	R/W	–	–	–	R/W*1	R/W*1
[Definição de transferência de dados para programação automática do livro de endereços]	R/W	–	–	–	R/W	R
[Manutenção]	R/W	–	–	–	–	–
[Central Address Book Management]	R/W	–	–	–	–	–

*1 Se a opção [Restringir adição de destinos utilizadores] da [Segurança Avançada] estiver definida como [Ligado] e se aplicar autenticação básica ao equipameno, cada utilizador pode alterar a palavra-passe apenas da sua própria conta.

Web Image Monitor: Central Address Book Management

Estas definições pertencem a [Gestão de equipamentos].

Estas definições não são apresentadas no caso de possuir privilégios de administrador. Nesse caso, especifique-as acedendo à [Gestão de equipamentos] > [Livro de endereços].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Central Address Book Management]	–	R/W	–	–	–	–

Web Image Monitor: Main Power Off

Estas definições pertencem a [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Main Power Off Mode]	–	R/W	–	–	–	–
[OK]	–	R/W	–	–	–	–

Web Image Monitor: Apagar trabalho da impressora

Estas definições pertencem a [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Apagar trabalho atual]	–	R/W	–	–	–	–
[Apagar todos os trabalhos]	–	R/W	–	–	–	–

Web Image Monitor: Reiniciar sistema

Estas definições pertencem a [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Reiniciar sistema]	–	R/W	–	–	R/W	–

Web Image Monitor: Gestão da Página Principal

Estas definições pertencem a [Gestão de equipamentos].

Quando a autenticação de administrador está definida, as restrições às operações de utilizador variam dependendo das configurações em "Definições disponíveis".

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Editar ícones]	R	R/W	R	R	R/W	R
[Repor visualização de ícones predefinida]	–	R/W	–	–	R/W	–
[Definições do ecrã principal]	R	R/W	R	R	R/W	R

Web Image Monitor: Monitorização do ecrã

Estas definições pertencem a [Gestão de equipamentos].

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Visualizar ecrã do equipamento]	–	R/W	–	–	–	–

Web Image Monitor: Personalizar ecrã por utilizador

Aparece se [Personalização do utilizador] estiver definido como [Permitir].

Os utilizadores apenas podem alterar as suas próprias definições.

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Editar ícones]	–	–	–	–	–	R/W
[Repor visualização de ícones predefinida]	–	–	–	–	–	R/W
[Prioridade de função por utilizador]	–	–	–	–	–	R/W

Web Image Monitor: Servidor de documentos

Estas definições encontram-se em [Trb impr/Fich guardado].

O que os utilizadores podem fazer com os seus ficheiros guardados depende dos respetivos privilégios de acesso. Para obter detalhes, consulte Pág. 334 "Lista de Privilégios de Operação para Ficheiros Guardados".

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Nova pasta]	–	–	–	R/W	R/W	R/W
[Editar pasta]	–	–	–	R/W	R/W	R/W
[Apagar pasta]	–	–	–	R/W	R/W	R/W
[Desbloquear pasta]	–	–	–	R/W	–	–
[Imprimir]	–	–	–	–	R/W	R/W
[Enviar]	–	–	–	–	R/W	R/W
[Apagar]	–	–	–	R/W	R/W	R/W
[Editar informações detalhadas]	–	–	–	R/W	R/W	R/W
[Download]	–	–	–	–	R/W	R/W
[Desbloquear ficheiro]	–	–	–	R/W	–	–

Web Image Monitor: Impressora: Trabalhos de impressão

Estas definições encontram-se em [Trb impr/Fich guardado].

Os documentos da impressora que podem ser geridos por utilizadores são aqueles que os próprios utilizadores guardaram ou aqueles que não necessitam de autenticação de utilizador.

Os documentos guardados por outros utilizadores não são apresentados.

Definições	Utilizador	Equip.	Rede	Fich.	Remov.	Def.
[Imprimir]	–	–	–	–	R/W *1	R/W *1
[Apagar]	–	–	–	R/W	R/W *1	R/W *1
[Editar informações detalhadas]	–	–	–	R/W	R/W *1	R/W *1
[Desbloquear trabalho]	–	–	–	R/W	–	–

*1 O acesso a documentos guardados pode ser restringido, dependendo dos privilégios de acesso do utilizador.

Lista de Privilégios de Operação para Ficheiros Guardados

Compreender os cabeçalhos

- Ler

  Utilizadores com privilégios de leitura.
- Editar

  Utilizadores com privilégios de edição.
- E/E

  Utilizadores com privilégios de edição/eliminação.
- Completo

  Utilizadores com privilégios de controlo total.
- Proprietário

  Indica o utilizador que registou um documento ou o utilizador especificado como proprietário.
- Fich.

  Indica o administrador de ficheiros.

Compreender os símbolos

R/W: Pode executar

–: Não pode executar

Definições	Ler	Editar	E/E	Completo	Proprietário	Fich.
[Impressão]	R/W	R/W	R/W	R/W	R/W	–
[Detalhes]	R/W	R/W	R/W	R/W	R/W	R/W
[Pré-visualização]	R/W	R/W	R/W	R/W	R/W	–
[Alt. privil. acesso]: [Proprietário]	–	–	–	–	–	R/W
[Alt. privil. acesso]: [Permissões p/ Utiliz./Grupos]	–	–	–	R/W	R/W*1	R/W
[Alterar nome fich.]	–	R/W	R/W	R/W	R/W*1	–
[Alt. palavra-passe]	–	–	–	–	R/W	R/W
[Desbloq. ficheiros]	–	–	–	–	–	R/W

Definições	Ler	Editar	E/E	Completo	Proprietário	Fich.
[Apagar ficheiro]	–	–	R/W	R/W	R/W*1	R/W
[Impr pág especific]	R/W	R/W	R/W	R/W	R/W*1	–

*1 O proprietário pode alterar os privilégios de operação.

Lista de Privilégios de Operação para Livros de Endereços

Compreender os cabeçalhos

- Ler

  Utilizadores com privilégios de leitura.

- Editar

  Utilizadores com privilégios de edição.

- E/E

  Utilizadores com privilégios de edição/eliminação.

- Completo

  Utilizadores com privilégios de controlo total.

- Entrada

  Indica um utilizador cujas informações pessoais estão registadas no livro de endereços. Indica ainda qualquer utilizador que saiba o respetivo nome e palavra-passe de início de sessão.

- Utilizador

  Indica o administrador de utilizadores.

Compreender os símbolos

R/W: É possível executar, alterar e ler.

R: É possível ler.

–: Não é possível executar, alterar, nem ler.

[Nomes]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[Nome]	R	R/W	R/W	R/W	R/W	R/W
[Nome visualizado]	R	R/W	R/W	R/W	R/W	R/W
[N.º de registo]	R	R/W	R/W	R/W	R/W	R/W
[Prioridade visualização]	R	R/W	R/W	R/W	R/W	R/W
[Selecionar título]	R	R/W	R/W	R/W	R/W	R/W

[Info. Autent.]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[Código utilizador]	–	–	–	–	–	R/W
[Nome utiliz. início sessão]	–	–	–	–	R	R/W
[Pal-passe início sessão]	–	–	–	–	R/W*1	R/W*1
[Autenticação SMTP]	–	–	–	–	R/W*1	R/W*1
[Autenticação da pasta]	R	R/W*1	R/W*1	R/W*1	R/W*1	R/W*1
[Autenticação LDAP]	–	–	–	–	R/W*1	R/W*1
[Funções disponíveis]	–	–	–	–	R	R/W
[Limit volumes utiliz impr]	–	–	–	–	R	R/W

*1 Não é possível ler palavras-passe.

[Proteção]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[Utilizar nome como]	R	R/W	R/W	R/W	R/W	R/W
[Proteger destino] [Código de proteção]	–	–	–	R/W *2	R/W *2	R/W *2
[Proteger destino] [Objeto de proteção]	–	R/W	R/W	R/W	R/W	R/W
[Proteger destino] [PermissõesUtiliz/Grupos]	–	–	–	R/W	R/W	R/W
[Proteger ficheiro(s)]: [PermissõesUtiliz/Grupos]	–	–	–	R/W	R/W	R/W

*2 Não é possível ler o código de [Código de proteção].

[Enviar e-mail]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[Endereço de e-mail]	R	R/W	R/W	R/W	R/W	R/W

[Pasta]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[SMB/FTP/NCP]	R	R/W	R/W	R/W	R/W	R/W
[SMB]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Nome servidor]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Nº porta]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Tipo de ligação]	R	R/W	R/W	R/W	R/W	R/W
[Teste de ligação]	R	R/W	R/W	R/W	R/W	R/W

[Adic. ao grupo]

Definições	Ler	Editar	E/E	Completo	Entrada	Utilizador
[N.º de registo]	R	R/W	R/W	R/W	R/W	R/W
[Procurar]	R	R/W	R/W	R/W	R/W	R/W
[Mudar título]	R/W	R/W	R/W	R/W	R/W	R/W

Nota

- Quando a opção [Restringir adição de destinos utilizadores] da [Segurança Avançada] está definida como [Ligado], independentemente dos privilégios de operação do utilizador, apenas o administrador de utilizadores pode aceder ao livro de endereços.

ÍNDICE

A

Administrador..... 12
Alterar estrutura do firmware..... 238
Apagar auto memória..... 85
Apagar toda a memória..... 89
Assinatura eletrónica..... 120
Ativar/desativar protocolos..... 96
Atualizar firmware..... 238
Autenticação básica..... 34
Autenticação de trabalhos da impressora..... 53
Autenticação de utilizador..... 28
Autenticação do utilizador..... 29
Autenticação Kerberos..... 40, 154
Autenticação LDAP..... 48
Autenticação NTLM..... 40
Autenticação por código de utilizador..... 32
Autenticação utilizando um dispositivo externo. 63
Autenticação Windows..... 39
Autenticar trabalho atual..... 237
authfree..... 55

B

Bloquear modo de assistência técnica..... 243

C

Certificado intermédio..... 111
Certificado próprio..... 108
Chave de encriptação..... 81
Chave de encriptação do driver..... 234
  Grau de encriptação..... 234
Código de encriptação do driver..... 151
Código de erro..... 253
Comandos de definição telnet IPsec..... 138
Controlo de acesso..... 95
Criação de um certificado do dispositivo..... 109

D

Definições da chave de encriptação negociada automaticamente..... 127
Definições de código de encriptação negociado automaticamente..... 133
Definições em SNMPv1, v2..... 236
Definições IPsec..... 127
Digitalizar para dispositivos de armazenamento amovível..... 72

E

Encerramento automático de sessão..... 61
Encerrar sessão(Administrador)..... 22
Encriptação de dados (Disco rígido)..... 77
Encriptação de dados (livro de endereços)..... 75
Encriptação de e-mail..... 118
Encriptar definições personalizadas do utilizador e livro de endereços..... 235

F

Função de bloqueio da palavra-passe..... 58
Funções de segurança avançadas..... 234
Funções disponíveis..... 70
Funções do browser..... 222

G

Gestão do ficheiro de registo - Web Image Monitor..... 178

I

IEEE 802.1X..... 144
  Certificado de dispositivo..... 145
  Certificado externo..... 144
  Ethernet..... 145
  wireless LAN..... 147
Impressão bloqueada..... 170
Imprimir a partir de dispositivos de armazenamento amovível..... 72
Informação sobre segurança avançada..... 244
Informações de autenticação para iniciar sessão..... 37
Informações de registo..... 178
Iniciar sessão(Administrador)..... 20
Instalação de certificados de dispositivo..... 110
IPsec..... 125

M

Melhorar proteção de ficheiros..... 235
Mensagem de erro..... 251
Modo de encriptação SSL/TLS..... 115

N

Nível de segurança da rede..... 102

P

Palavra-passe de autenticação IPP..... 152
Palavra-passe para ficheiros guardados.....161
Palavras-passe transmitidas..... 151
PDFs com assinaturas eletrónicas..... 124
Permissão de acesso a ficheiros guardados.....161
Permissão de acesso ao livro de endereços.....73
Política da palavra-passe.....237
Privilégios de administrador..... 14
Privilégios de operação.....269
Problemas operacionais.....264
Proteção de menus.....68
Protocolo AH..... 126
Protocolo AH + Protocolo ESP..... 126
Protocolo ESP..... 126

R

Registo de administrador.....16
Remote Service.....237
Restringir adição de destinos de utilizadores... 236
Restringir utilização de destinos.....236
Restringir visualiz. informações utilizador..... 235

S

S/MIME..... 118
Segurança para a função de scanner..... 242
SNMPv3..... 150
SSL para ligações SMTP..... 116
SSL/TLS.....112
Substituir dados..... 85
Supervisor..... 23

U

Utilização de slot para dispositivos de armazenamento amovível.....72
Utilizadores.....27

V

Validade do firmware.....242
Verificação do estado do sistema..... 242

 © 2014